Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks

Good Practice Note

IFC International Finance Corporation
WORLD BANK GROUP
Creating Markets, Creating Opportunities

2121 Pennsylvania Avenue, N.W.
Washington, D.C. 20433
Internet: www.ifc.org

Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks

Good Practice Note

IFC International Finance Corporation
WORLD BANK GROUP
Creating Markets, Creating Opportunities

Table of Contents

Foreword

In recent years, simultaneous increases in reserve capital requirements, Anti-Money Laundering and Countering the Finance of Terrorism (AML/CFT) compliance requirements have created a marked increase in cost and complexity to banks globally. While many of these regulatory changes have increased financial system resilience and helped battle financial crime, they have also put increased pressure on correspondent banking relationships and cross border financial networks. These networks make trade possible, support remittances, and facilitate foreign currency settlements.

Faced with orders for corrective action, deferred prosecution agreements, and punitive financial fines issued by regulators, correspondent banks have responded by limiting their activities to markets with more acceptable regulatory risk-reward economic benefits.

The regulatory challenges and commercial economic factors in many of the emerging markets, particularly the smaller economies, have resulted in a disproportionate increase in costs and implementation challenges, exacerbated by the impact of withdrawal of the corresponding banking relationships. There has been a notable concentration of flows within trade lines and remittance channels, undermining smaller local banks which can be critical to financial sector stability and the growth and prosperity of emerging market countries.

IFC's study and publication, "De-Risking and Other Challenges in the Emerging Market Financial Sector,"[1] highlighted that over 25 percent of 300-plus banks in over 90 emerging markets reported correspondent bank relationship losses. Seventy-two percent of the banks covered by the study reported that they face exogenous challenges – primarily correspondent banking stress and related compliance challenges – that have touched every surveyed market irrespective of size or risk.

There is a compelling business case to be made for upgrading a bank's AML/CFT capabilities. Banks that lead the way in emerging markets are in stronger positions to maintain and/or grow their cross-border correspondent banking networks, putting them in a position to better serve customers and their respective connections to the global economy. This provides unique growth opportunities for their business, strengthening their market presence and stability. It opens doors to deeper data – driven innovation for viewing their markets, customers and product potential, which shifts their own individual growth curve.

As expectations for continuous improvement in AML/CFT compliance pervades the global financial system, it is important that EM financial institutions: (i) understand the business implications of ML/FT along with implications for security and criminality; (ii) identify additional compliance requirements for participating in the global financial system and (iii) find their own path to excellence in this area. We recognize that each country and each institution is different – each will need different levels of support or clarity as they work to achieve these goals. However, in many cases, the request is for guidance across several fronts: basic AML/CFT concepts, interpreting and implementing regulatory guidance, correspondent bank reporting and systems alignment, interpreting US/EU regulatory requirements, and technology-based solutions.

It is our belief that this publication can provide a measure of guidance, and that it can spur additional solutions opportunities to address the challenges currently faced by cross border financial networks. It is my hope that, as each financial institution stretches to address this issue, the attention to quality and excellence as well as the opportunity for innovation embedded in the collective effort will provide for an even stronger EM global financial system.

Paulo de Bolle, Senior Director
Global Financial Institutions Group

[1] http://documents.worldbank.org/curated/en/895821510730571841/pdf/121275-WP-IFC-2017-Survey-on-Correspondent-Banking-in-EMs-PUBLIC.pdf

Acknowledgments

Under the supervision of Manuela Adl and Cameron Evans, this Good Practice Note was prepared with contributions from Ebrahim Farouk, Annetta Cortez, Yannick Stephant, Susan Starnes, Robert Heffernan, Brian Robert Sokoliuk, Margarete O. Biallas, Mariyam Zhumadil, William C. Hayworth, Matthew Huggins, Sokhareth Kim, Elizabeth Gibbens, Andrew Berghauser, Lauren Kaley Johnson, and Rob Wright.

IFC would like to thank our colleagues and partners who reviewed and provided the insightful comments for the document including Yan Liu, IMF Assistant General Counsel, Emile J. M. Van Der Does De Willebois, World Bank Lead Financial Sector Specialist, John T. Murray, BONY-Mellan, Ayo Omoogun, Standard Chartered Bank,William L. Burmeister, Citibank, Lisan Hannah, The Bank of Nova Scotia, Lauren Girard and Jeff Gontero, JP Morgan Chase, Steven Puig, Banco BHD Leone, and Miriam Ratkovicova, Deloitte Transactions and Business Analytics LLP, without their input, this publication would not have been materialized.

Abbreviations of Common Terms

AM L	Anti-money laundering
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CBR	Correspondent banking relationship
CDD	Customer due diligence
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
CPMI	The Committee on Payment and Market Infrastructures
CFT	Combating the financing of terrorism
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FIU	Financial intelligence unit
FSB	Financial Stability Board
FT	Financing of terrorism
GPN	Good Practice Note
IFC	International Finance Corporation
IMF	International Monetary Fund
KRI	Key risk indicators
KYC	Know your customer
KYCC	Know your customer's customer
ML	Money laundering
MTO	Money transfer operators
PEP	Politically exposed person
STR	Suspicious-transaction report
WBG	World Bank Group

Chapter 1
Introduction

Background

The International Finance Corporation (IFC) is the private sector arm of the World Bank Group (WBG) and one of the leading investors and lenders in emerging markets. IFC's vision is that people should have the opportunity to escape poverty and improve their lives. IFC's purpose is to promote open and competitive markets in developing countries, support companies and other private sector partners, generate productive jobs, and deliver basic services. IFC's belief is that inclusion of emerging markets in the global economy is critical for building strong global financial systems.

Efforts to strengthen the global financial system following the 2007-2008 global financial crisis have contributed to withdrawal of correspondent banking services, which has a disproportionately negative impact on emerging markets. In the 2017 Correspondent Banking in Emerging Markets Survey[2] of over 300 banking clients in 92 countries, more than a quarter of global survey participants claimed reductions in correspondent banking relationships (CBRs). Increasingly, correspondent banks are paying greater attention to their respondents' Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) program effectiveness, Know Your Customer and Customer Due Diligence (KYC/CDD) programs, and their jurisdiction-related obligations to comply with AML/CFT requirements.[3]

In the Survey, private sector emerging market banks identified assistance with understanding and adapting to new global standards as one solution component that would be most useful. In response, IFC has published this Good Practice Note: AML/CFT Risk Management in Emerging Market Banks (GPN) for banks to advance their knowledge and capabilities in AML/CFT risk management and facilitate and support the maintenance of CBRs.

[2] IFC. 2018. De-Risking and Other Challenges in the Emerging Market Financial Sector.
[3] The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

De-Risking and its Impact on Emerging Markets

For simplicity, this GPN defines correspondent banking as an "arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks."[4] Correspondent banking facilitates banking services and is critical to international economic infrastructure. Some of the banking services and products affected by reductions in correspondent banking are listed in the table that follows.

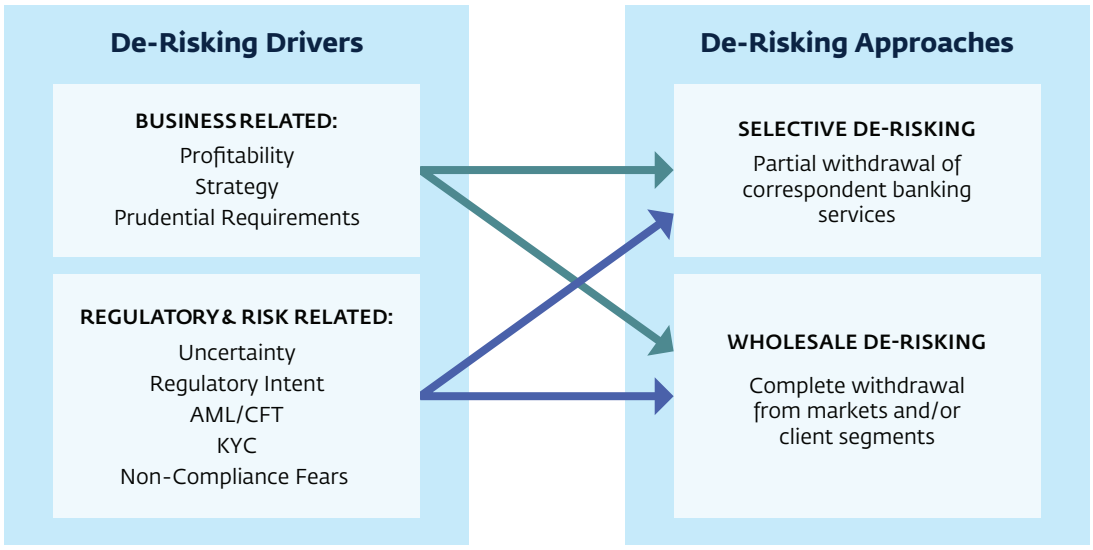
Primary Products / Services:	Secondary Products/Services:
• *Clearing and settlement*	• *Investment services*
• *International wire transfers*	• *Structured finance/ foreign investment*
• *Cash management services*	• *Securities =custody services*
• *Trade finance/credit letters and documentary collections*	• *Cross-border lending*
• *Foreign exchange services*	• *Check clearing*

Correspondent banking relationships play a key role in linking emerging market banks and their customers to the global financial system. Through these contractual relationships, emerging market banks (often in the role of respondents) gain access to financial services in foreign jurisdictions and provide cross-border payment services to their customers, ultimately promoting inclusion in the global financial system.

In recent years, a decline in correspondent banking relationships known as "de-risking" has become apparent. According to the Financial Action Task Force (FATF), de-risking refers to the "phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, AML/CFT risk in line with the FATF's risk-based approach."[5] The de-risking trend appears to affect the smallest and poorest countries in emerging markets more severely, although none are immune. A recent publication issued by IFC indicates that Sub-Saharan Africa, North Africa, Middle East, Latin America and the Caribbean, and Europe and Central Asia, are among the regions that most frequently reported a decline in correspondent banking relationships.[6]

The factors contributing to the termination of correspondent banking relationships are multiple and interrelated. As shown in Box 1, the drivers of de-risking can be grouped into two categories: business related and regulatory and risk related. The drivers may lead to either a complete withdrawal from markets, banks, and/or client segments or selective de-risking in the form of a partial withdrawal of correspondent banking services.

Box 1



Source: Excerpt from The Bankers Association for Finance and Trade (BAFT), De-Risking: How to address the de-risking dynamics?

[4] CPMI. 2015. A glossary of terms used in payments and settlement systems.
[5] http://www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-and-de-risking.html
[6] IFC. 2017. De-Risking and Other Challenges in the Emerging Market Financial Sector.

The ongoing evolution of higher AML/CFT risk management standards at the regional, national, and sometimes subnational level has created increasing ambiguity as well as inconsistent expectations. This environment has increasingly challenged developed market and emerging market banks in appropriately implementing risk-based controls and determining their reasonable risk appetite. For example, in 2016, to provide additional clarification on customer due diligence for correspondent banking relationships, FATF stated that banks are not required to conduct customer due diligence on the customers of their customers (known as KYCC). Despite these efforts to clarify customer due diligence requirements, some global banks remain concerned about the clarity of regulatory expectations and the liability associated with failure of their own AML/CFT risk management systems and processes that fully meet regulatory standards. The uncertainty around due diligence on a customer's customer makes it difficult for correspondent banks to assess the risk associated with respondent banks and motivates them to terminate some of these relationships.[7]

Increasing compliance costs have also affected the risk reward calculation for offering and maintaining correspondent banking relationships. Some of these costs, such as operational ones, are easy to quantify. Other costs, such as reputational impact of potential enforcement actions, are harder to assess. Many banks recognizing the business need are instituting global best practices and investing in new processes and systems to more efficiently and effectively manage AML/CFT risk. Some of these investments include detailed KYC databases, systems enabling ongoing monitoring of their customer's transactions, and investigating, as appropriate, unusual and potentially suspicious transactions.

A decline in correspondent banking relationships has been a concern for emerging market countries for some time given that this trend appears to negatively affect trade, putting at risk the import and export of critical goods and ultimately economic growth.8 In the Caribbean for example, countries heavily rely on trade and cross-border payments to the extent that in 2014, Caribbean countries' external trade accounted for 94 percent of those countries' collective GDP. Additionally, these countries heavily rely on the import of large portions of their essential food, energy, and medical supplies.

The WBG's paper that summarizes the main observations of the eight country case studies conducted in 2017 suggests that money transfer operators (MTOs) have been particularly affected. In almost all surveyed countries, a number of respondent banks have been instructed by their correspondent banks to stop servicing MTOs. Cross-border financial services provided by MTOs are used intensively in emerging markets. The flow of funds from migrant workers to their home countries is an important source of income in many emerging economies.[9] The decline in CBRs can negatively affect remittances and the ability of families in emerging markets to receive income they depend on.

The IFC's purpose in publishing this GPN is to provide practical guidance and information to assist emerging market banks in profitably providing cross-border services to their clients, managing their correspondent relationships more effectively, maintaining their existing CBRs to avoid de-risking, and facilitating opening of new CBRs.

In September 2018, IFC published "Navigating Essential Anti-Money Laundering and Combating the Financing of Terrorism Requirements in Trade Finance: A Guide for Respondent Banks" to increase respondent banks' awareness of AML/CFT requirements and developments as they related to trade finance. Similar to the GPN, this guide is intended to assist emerging market banks in securing and retaining CBRs. Both publications are intended to assist emerging market banks in developing and revising their risk management strategies, with the former providing guidance related to a robust enterprise-wide AML/CFT program and the latter mainly focusing on AML/CFT developments related to trade finance.

Other organizations, such as the World Bank, International Monetary Fund (IMF), and Financial Stability Board (FSB), are also monitoring developments and analyzing the impact

7 CPMI. 2016. Correspondent Banking.
8 IFC. 2018. De-Risking and Other Challenges in the Emerging Market Financial Sector.
9 The World Bank Group. 2017. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

of the decline in CBRs. The GPN is unique in that it is in response to our clients' requests and aims to be a practical guide that may help mitigate some of the negative impacts of de-risking while adding to the many initiatives undertaken by the international community to address de-risking.[10]

About This Good Practice Note

This GPN synthesizes current international AML/CFT standards and guiding principles in a practical format to assist banks in emerging markets in effectively implementing the desired good practices that will enhance the maintenance of CBRs.

Why Should a Bank like Yours Invest in the Development of a Robust AML/CFT Program?

A robust AML/CFT program requires a substantial investment because it calls for not only a sufficient number of experienced resources but also for advanced technology that can support the bank's AML/CFT compliance function to better identify, measure, monitor, control, and report on Money Laundering/Financing of Terrorism (ML/FT) risks. So why should a bank like yours want to make this investment?

Having a robust AML/CFT program offers multiple benefits to your bank. Consider that:

- An AML/CFT program can mitigate the risk faced by a correspondent bank in doing business with you if your bank is located in a high-risk jurisdiction and can bring the overall residual risk to a level acceptable to your correspondent banks.
- Your ability to obtain and retain CBRs will enable your bank to provide the full spectrum of offshore banking services demanded by your high-value banking customers.
- If your correspondent bank is satisfied with your customer due diligence standards, it will likely be receptive to providing payable-through-accounts services you may need.
- Having robust systems and technologies will provide your bank with required capabilities to participate in KYC utilities used by some large correspondent banks. Such KYC utilities have the potential to improve efficiency and lower costs because of a lesser amount of documentation being exchanged. Lower costs have the potential to make CBRs more attractive for correspondent banks that have indicated these relationships have become unprofitable. Additionally, new technologies may lower your own compliance costs over the long run.
- Failure to have an effective AML/CFT compliance program can result in enforcement action from the supervisory authorities that generally include large fines in addition to:
    - Heightened regulatory scrutiny;
    - Pressure on the bank's funding and liquidity;
    - Costly remediation efforts and high legal costs;
    - Civil and criminal liability of the board of directors/senior management/other employees;
    - Shareholder lawsuits against board of directors/senior management for lack of oversight and negligence;
    - Reputational damage;
    - Lack of foreign direct investments; and
    - Higher cost of borrowing in the international arena.

[10] Refer to Annex 2 for a list of recent work related to correspondent banking conducted by different international bodies.

THIS GOOD PRACTICE NOTE WILL

- *Highlight the business case for respondent banks to invest in an improved AML/CFT risk management program.*
- *Interpret for emerging market bank professionals the AML/CFT guiding principles and standards published by various international bodies, including FATF, the Basel Committee on Banking Supervision (or BCBS), and the Wolfsberg Group.*
- *Increase emerging market banks' awareness of AML/CFT expectations of U.S. and European regulators that oversee many of their correspondent banks.*
- *Describe what is expected of emerging market banks implementing an AML/CFT risk management program.*
- *Highlight where new technologies and operating models may be deployed to enhance emerging market banks' AML/CFT programs.*
- *Provide real-world examples and case studies that can be used by banks to enhance their AML/CFT programs.*
- *Outline a process for self-assessment of the maturity level of an emerging market bank's AML/CFT program.*
- *Provide insight into the potential impediments to an emerging market bank's effective AML/CFT program.*

This Good Practice Note will not

- *Interpret regulatory requirements and expectations imposed by national and/or local regulators in emerging markets.*
- *Provide a one-size-fits-all solution that can be deployed by any emerging market bank; instead best practices discussed in this GPN should be tailored to the banks' risk profile and the overall risk management framework.*

This GPN is organized as follows:

Chapter 1	Introduces the GPN, its role and objectives, de-risking phenomena, impact on correspondent banking services, and emerging markets.
Chapter 2	Introduces the foundational concepts and importance of establishing a strong enterprise risk management framework and links the establishment of the AML/CFT program component within this risk framework.
Chapter 3	Establishes the core of the AML/CFT program within a bank and provides details of the key elements of a bank's AML/CFT internal controls.
Chapter 4	Supports the bank in establishing a dialogue with its correspondent bank and other stakeholders, such as supervisors, to develop a shared view of requirements and capabilities.
Chapter 5	Establishes the foundation for an internal controls assessment tool and introduces a high-level maturity matrix measuring and/or documenting the strength of internal controls.
Chapter 6	Summarizes the critical elements of the GPN and guidance on how best to manage CBR relationships.

An AML/CFT risk management program is one of many components of an institution's overall risk management framework, which includes various risk categories, such as credit risk, interest rate risk, operational risk, compliance risks, and reputational risk, to name a few. An effective risk management framework is fundamental to a safe and sound financial institution, jurisdiction financial system, and ultimately the integrity of the international financial system. Although this GPN briefly discusses the link between a bank's overall risk management framework and other financial crime risks (including AML/CFT, fraud, antibribery and corruption, market manipulation and tax evasion risks), **its main focus is on the development and enhancement of the AML/CFT compliance component.**

Chapter 2

Establishing a Sound Financial Institution Risk Management Framework, Governance Structure, and Culture

Introduction

Taking risk is fundamental to the business of banking. Successfully managing those same risks is critical to profitable and sustainable banking. Establishing a strong risk management framework for the range of risks encountered by a bank is essential for its safe and sound operation. A formal risk management program creates the framework for identifying, measuring, monitoring, reporting, and ultimately addressing risks. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Framework is one example of an internationally accepted framework. It is similar to other international risk management guidances from the Basel Committee on Banking Supervision (BCBS), International Organization for Standardizations (ISO), and others.[11]

A strong risk management framework sets the foundation for establishing a robust AML/CFT program. Regardless of size and complexity, a bank must have effective risk management programs appropriately designed to the organization's products, services, customers and overall risk profile. Adequate risk management frameworks can vary considerably in sophistication based on the bank's business strategy, markets, and risk profile but are ultimately judged by their effectiveness in managing risk across all a bank's operations.

The principles of sound risk management apply to the entire spectrum of risks facing a financial institution, including, but not limited to business/strategic, market, credit, liquidity, operational, legal, reputational, and compliance risk[12], each of which is best described as follows:

- ***Business/Strategic risk*** *is the risk that affects or is created by an organization's business strategy and strategic objectives.*
- ***Market risk*** *is the risk to a bank's financial condition resulting from adverse movements in market rates or prices, such as interest rates (for example, interest rate risk), foreign exchange rates, or equity prices.*
- ***Credit risk*** *arises from the potential that a borrower or counterparty will fail to perform on an obligation.*
- ***Liquidity risk*** *is the potential that an institution will be unable to meet its obligations as they come due because of insufficient funds or an inability to liquidate assets or obtain adequate funding, or that it cannot easily unwind or offset specific exposures without significantly affecting its balance sheet/capital levels, in some cases as a result of lowered market prices because of inadequate market depth or market disruptions.*
- ***Operational risk*** *arises from inadequate or failed internal processes, people, and systems or from external events. Examples include inadequate information systems, operational execution problems, breaches in internal controls, fraud, or unforeseen external catastrophes that result in unexpected losses.*
- ***Legal risk*** *arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization.*
- ***Reputational risk*** *is the potential that negative publicity regarding an institution's business practices, whether*

[11] "Enterprise Risk Management—Integrating with Strategy and Performance;" June 2017. Committee of Sponsoring Organizations of the Treadway Commission (COSO). https://www.coso.org/Pages/erm.aspx; Sound management of risks related to money laundering and financing of terrorism;" June 2017. Basel Committee on Banking Supervision (BCBS); https://www.bis.org/bcbs/publ/d405.htm; "Risk Management – Guidelines, ISO 31000:2018;" International Organization for Standardizations (ISO). https://www.iso.org/iso-31000-risk-management.html

[12] Board of Governors of the Federal Reserve System SR 95-51.

true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.

- *Compliance risk is exposure to legal penalties, financial forfeiture and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.*

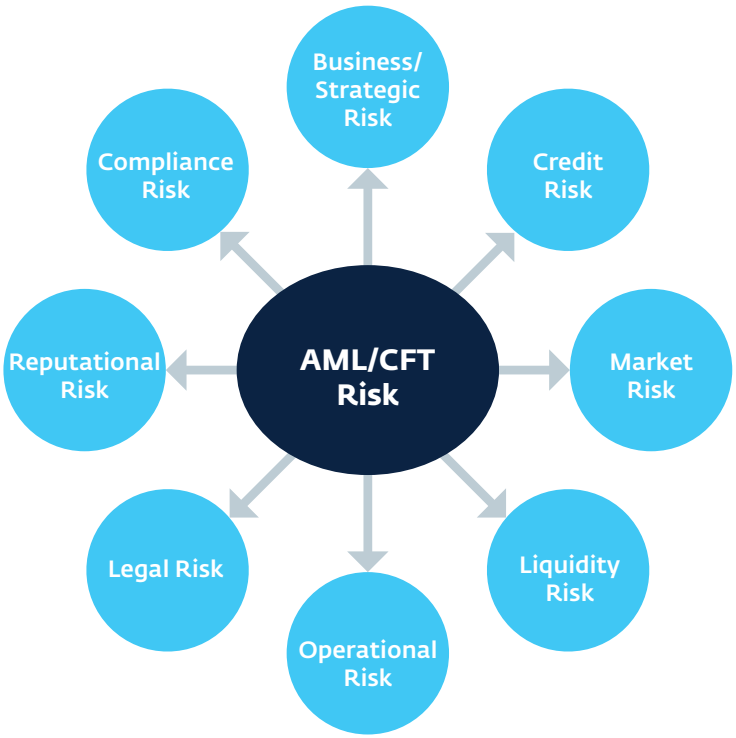
AML/CFT risks are primarily incorporated within the Compliance or Legal risk category. AML/CFT risks can also affect multiple risk categories, including liquidity, strategic, operational, legal/compliance, reputational, and in some instances credit risk. The Board, Chief Risk Officer (CRO), and senior management must monitor the range of AML/CFT risk across the organization to ensure it remains within the defined risk appetite parameters.

From a risk management perspective, before about 2005, AML/CFT compliance shortcomings generally did not trigger substantive civil and criminal enforcement actions against banks. Over the last 10 years there has been an increasing emphasis on AML/CFT compliance, civil enforcement actions, civil penalties, and criminal prosecutions (deferred and not deferred). This change in emphasis and approach to enforcement of relevant regulations was a result of governments viewing AML/CFT compliance as part of the jurisdiction's national security infrastructure versus the earlier view of AML/CFT compliance as more of a bank internal matter. This shift of prominence and approach to risk management expectations has had substantial effects within jurisdictions as well as across the globe's financial activities. For example, increasing compliance costs, new risk/reward calculation for financial relationships, and the resultant phenomena of de-risking.

This shift has affected several global banks, which have been subject to varying types of civil and criminal sanctions (financial penalties and remedial regulatory actions) and required to substantially enhance of their AML/CFT programs. In addition, FATF's new mutual evaluation standards, implemented in 2014, which include an effectiveness assessment, have increased pressure on emerging market jurisdictions to reassess and enhance portions of their own AML/CFT infrastructure and internal requirements. As a result, governments and financial sector supervisors worldwide have increasingly emphasized the importance of having a strong culture of AML/CFT compliance within their financial sector and its leadership, including the Board of Directors, senior management, middle management, and owners of banks regardless of size, complexity, or region.

This increasing emphasis and attention on compliance and financial and criminal penalties (including potential individual liability against AML officers and others) has impacted the cost of AML/CFT compliance and banks' risk appetites. It also had a direct follow-on affect in the provision of correspondent banking services (for example, de-risking).

Figure 1: AML/CFT Risk Relationship Chart



Compliance Risk Management

Firmwide compliance risk management[13] refers to processes used to manage compliance risk across an entire organization, both within and across business lines, support units, legal entities, and jurisdictions. This approach ensures that compliance risk management is conducted in a broader context than would occur solely within individual business lines of legal entities.

A bank's compliance risk management program should be documented in the form of compliance policies and procedures and compliance risk management standards.

As part of a bank risk management framework, regulatory and legal compliance is typically considered within either the Legal risk or Compliance risk category. Regardless, as banking organizations have greatly expanded the scope and global nature of their business activities, compliance requirements associated with these activities have become more complex. As a result, organizations are confronted with risk management and corporate governance challenges, particularly with respect to compliance risks that transcend business lines, legal entities, and jurisdictions. Many banking organizations have enhanced firmwide compliance risk management programs and program governance/ oversight. A firm-wide compliance function plays a key role in managing and overseeing compliance risk, including AML/CFT, while promoting a strong culture of compliance across the organization.

Elements of a sound compliance risk management system[14] include the following:

- *Active Board and senior management oversight (including emphasis on culture to ensure a balance is achieved between profit motive and risk taking, and compliance across all categories[15]);*
- *Comprehensive risk measurement, monitoring, and management information systems; and*
- *Comprehensive internal controls, including adequate policies, procedures, and limits.*

Active Board and Senior Management Oversight

Effective risk management is a central element of proper corporate governance. In particular, the requirement for the Board of Directors to approve and oversee the policies for risk, risk appetite, internal controls, and compliance is appropriate for ML/FT risk. The board of directors must establish an infrastructure to fully identify risk, monitor risk exposures, ensure sufficiency of the internal control environment implemented to manage the unique risks of the bank, and actively engage with leadership and bank personnel concerning the organization's culture. These include:

- *Developing business strategy and organizational goals that promote and communicate organizational culture (that is, tone at the top). Culture describes what a group does as opposed to what it says it does. The "control environment" is the organization's culture. It can be inferred from observable behaviors and a description of prevalent relationships.*
- *Identifying and hiring qualified senior management.*
- *Establishing risk appetites and a risk framework, including policies and procedures.*
- *Monitoring operational performance.*
- *Aligning business strategy as the business environment evolves.*

At the best banks, AML/CFT risk management is regarded as an integral part of a bank's risk and compliance management framework. Information about AML/CFT risk is communicated to the Board in a timely, complete, understandable and accurate manner so that the board is equipped to make informed decisions. Explicit responsibility is allocated by the Board of Directors, establishing the governance structure of the bank, for ensuring that the bank's policies and procedures are implemented and managed effectively. The Board and senior management generally appoint an appropriately qualified chief AML/ CFT officer having overall responsibility for the AML/CFT function. The chief AML/CFT officer must have the stature and necessary authority within the bank such that she/he has the necessary access to the Board, senior management, and business lines.

---

[13] Board of Governors of the Federal Reserve System SR 08-08/CA 08-11 October 16, 2008.
[14] COSO – Enterprise Risk Management Framework.
[15] Risk category examples include business/strategic, credit, market, liquidity, operational, compliance, legal, and reputational risk.

Although all Boards of Directors are ultimately responsible for bank strategy and operations, they also are responsible for ensuring that management is taking the necessary steps to identify, measure, monitor, and control these risks, retain the level of technical knowledge required to operate a bank, and communicate the proper culture.

Senior management is responsible for implementing strategies in a manner that manage risks associated with each strategy and ensures compliance with laws and regulations on a long-term and day-to-day basis. Accordingly, management should be fully involved in the activities of their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls, and risk monitoring systems are in place and that lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of and need for effective internal controls and high ethical standards. Meeting these responsibilities requires senior managers of a bank to have a thorough understanding of banking and financial market activities and detailed knowledge of the activities their institution conducts, including the nature of internal controls necessary to limit the related risks.

RISK MEASUREMENT, MONITORING, AND MANAGEMENT INFORMATION SYSTEMS

Effective risk monitoring requires identifying and measuring all material risk exposures. As such, risk monitoring activities must be supported by information systems that provide the CRO, senior management, and the Board with timely reports on the financial condition, operating performance, and risk exposure of the consolidated organization. Regular and sufficiently detailed reports for line managers (for example, first line) engaged in the day-to-day management of the organization's activities and for compliance managers (for example, second line) are also required.

Risk measurement, monitoring, reporting, and the technology that supports these processes has evolved over the past years. It is now critical that banks leverage data and various systems and technologies to support their AML/CFT compliance risk management program and program oversight. The use of technology will vary based on the size and complexity of the institution. The chief AML/CFT officer, however, should have access to and benefit from the IT system as far as it is relevant for his/her function, even if operated or used by other business lines.

Some of the key reports necessary for monitoring the operation of AML/CFT risk management operations are related to overall bank risk assessment, customer identification, periodic assessment and reassessment of higher-risk customers, performance of suspicious transaction monitoring and reporting systems, and trainings.

At a minimum, a bank should have a monitoring system in place that is suitable with respect to its size, activities, and complexity as well as the risks present in the bank. For most banks, especially those that operate across borders, effective monitoring is likely to require automation of the monitoring process.

An annual internal audit should evaluate the IT system to ensure that it is appropriate and used effectively by the first and second lines of defense.[16]

COMPREHENSIVE INTERNAL CONTROLS, INCLUDING POLICIES, PROCEDURES, AND LIMITS

After the Board and senior management have finalized their business strategy, quantified the risks within the institution, and determined their risk appetites (including limits), they then direct senior management to work on designing and implementing tailored policies, procedures, and controls for the risks that arise from the bank's activities and customers. Although all banking organizations should have policies and procedures that address their significant activities and risks, the coverage and level of detail embodied in these statements will vary.

At a minimum, banks are required to have a thorough understanding of the inherent ML/FT risks present in its customer base, products, delivery channels, and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business. Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately manage the identified inherent risks.

Internal Controls

It is well known that an institution's internal control structure is critical to the safe and sound functioning of the banking organization and its risk management system.

[16] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

Therefore, establishing and maintaining an effective system of controls, including the monitoring of official lines of authority and ensuring the appropriate separation of duties, is one of management's most important responsibilities.

The relationship between the internal audit, compliance, and risk management functions has gained greater regulatory scrutiny since the 2008 financial crises. Regulators worldwide have focused their attention on the role of internal audit and how it complements the overall risk management framework and how it assesses business line management, risk management, compliance, and other control functions. It is the expectation of regulators that a bank should have an effective risk management function, a compliance function, and an internal audit function. Each of these control functions, along with the bank's operational management, constitutes a **line of defense** against the risks the entity faces and are referred to as the three lines of defense.[17]

The three lines of defense are as follows:

- *First line:* ***operational management;***
- *Second line:* ***risk management function, compliance function, and other monitoring functions;*** *and*
- *Third line:* ***internal audit function.***

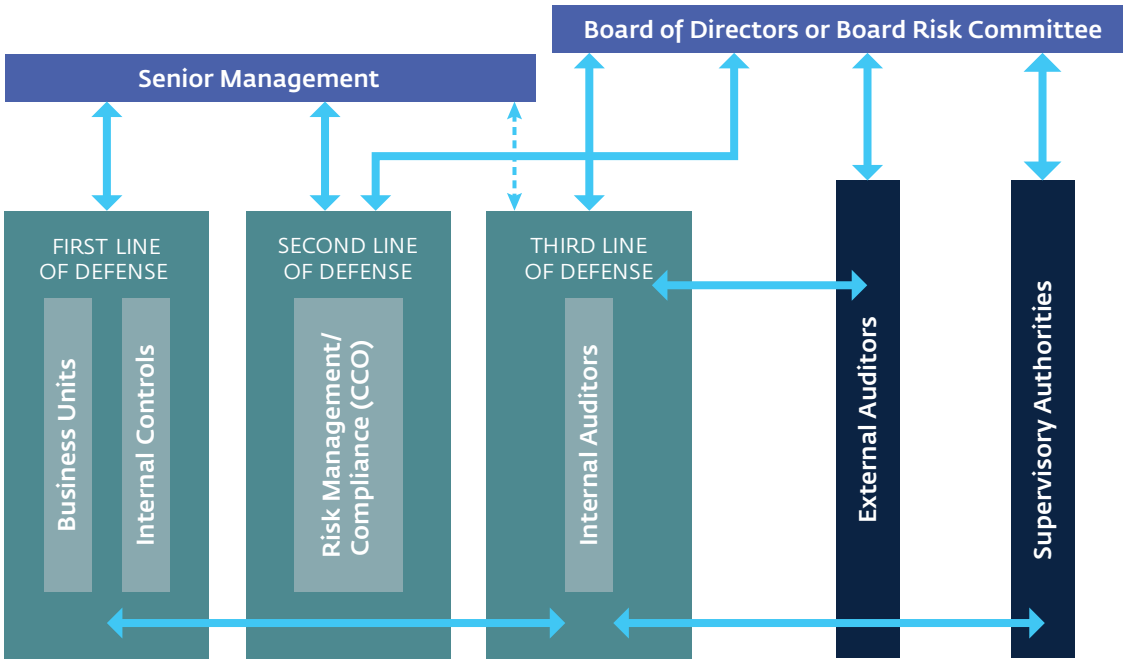
Risk Management and Compliance Oversight Structure: Model Illustration of the Three lines of Defense

The diagram that follows is an illustration of a risk management compliance oversight structure model[18]. The CRO and, for general compliance and AML/CFT controls, the Chief Compliance Officer (CCO) are part of the second line of defense, with the senior officer typically having operational responsibility for AML/CFT compliance. It should also be noted that in some banks, the CCO may be the chief AML/CFT officer.

In the context of overall risk management, the front office customer-facing business units are the first line of defense responsible for identifying, assessing, and managing the risks within their business areas. They should know and carry out the policies and procedures and be allotted sufficient resources to do so effectively.

The second line of defense are control functions that ensure policies and procedures are followed (for example, risk management, compliance, human resources, and legal). The risk management function facilitates and monitors the implementation of effective risk management practices by business-line management and reports exceptions and the status of first-line implementation.

Figure 2: Three Lines of Defense



[17] BCBS - The internal audit function in banks, December 2011; Principles for enhancing corporate governance, October 2010; Compliance and the

[18] Adapted from the European Confederation of Institutes of Internal Auditors / Federation of European Risk Management Associations Guidance on the 8th EU Company Law Directive, article 41.

The third line of defense is commonly referred to as the internal audit function. The internal audit function is responsible for assessing the effectiveness of the design and execution of internal control and compliance with laws, rules, and regulations. They also assess the work performed by the second line to ensure that both lines are performing as intended. Internal audit independently reports and provides periodic written assessment of the testing of controls and applicable legal compliance.

For AML/CFT risk management, the front office customer-facing business units continue to be responsible for identifying, assessing, and managing the risks within their business areas. (Given the evolving nature of AML/CFT expectations and requirements, it is common for the second line to support the first line regarding technical knowledge and to perform the AML/CFT risk assessment.) In today's environment, the AML/CFT second line, led by the appointment of the AML officer, not only performs second-line compliance testing responsibilities, which can be leveraged by the third line (internal audit), but also may operate some first line functions, including monitoring for suspicious activity, initial and ongoing screening of customer onboarding, and sanctions compliance screening. The unit should know and carry out the policies and procedures and be allotted sufficient resources to do so effectively. The AML/CFT third line of defense performs similar functions and has the same responsibilities as the institutional third line but is also responsible for this highly technical and risk-based compliance area.

FIRST LINE: OPERATIONAL MANAGEMENT

Operational management is responsible, and accountable for identifying, assessing, controlling, mitigating, and reporting on risks encountered during a bank's business activities.

This "first line" is also the business generator, responsible for defining risk-taking limits and following those limits, following policy guidelines, implementing/using approved procedures. First line is also instrumental, at high levels, in defining a bank's risk-taking limits Through a cascading responsibility structure, midlevel managers often design and implement detailed procedures that serve as controls and supervise execution of such procedures by their employees.

Employees in the first line are integral in AML/CFT compliance risk management through customer interactions, management of customer relationships, and execution of approved policies and procedures. The first line is critical for meeting one of the most important AML/CFT reporting responsibilities-- the identification of unusual and suspicious activity. During their day-to-day activities, first-line employees may observe unusual or potentially suspicious activity and/or behavior exhibited by customers. First-line employees are required, according to policies and procedures, to be vigilant in their identification, escalation, and reporting of potentially suspicious and or unusual activities. Management should ensure that all personnel, especially employees who directly interact with customers, adhere to the internal processes for identification and referral of potentially suspicious activity. Management must also be clear on the bank's response to suspicious activity beyond the referral including policies regarding exiting the client, communications with correspondent banks, and internal review of previous customer activity. A bank must have adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards are met. AML/CFT compliance is considered to be the responsibility of everyone within the organization.

Training of staff is critical. The scope and frequency of such training should be tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the bank. All banks should implement ongoing employee training programs so that bank staff are adequately trained to implement the bank's policies and procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank according to their needs and the bank's risk profile.

Training needs will vary depending on staff functions and job responsibilities. Training course organization and materials should be tailored to an employee's specific responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement the bank's AML/CFT policies and procedures. For the same reasons, new employees should be required to attend training as soon as possible. Refresher training should be provided to ensure that staff are reminded of their obligations and their knowledge and expertise are kept up to date.

SECOND LINE: RISK MANAGEMENT FUNCTION, COMPLIANCE FUNCTION, AND OTHER MONITORING FUNCTIONS

These are control functions that also ensure policies and procedures regarding risk-taking (risk management, compliance risk, human resources, and legal) are in place and enforced. The risk management function facilitates and monitors the implementation of effective risk management

practices by business-line management. It assists business-line management in defining risk exposures and risk reporting through the organization. The compliance function monitors the risk of noncompliance with laws, regulations, and standards. Other monitoring functions may include human resources and the legal department.

In most banks as part of the second line of defense, the chief AML/CFT officer has the responsibility for ongoing fulfillment of all AML/CFT duties by the bank. Depending on the size and complexity of the bank, the chief AML/CFT officer may also perform the function of the CRO or the CCO or equivalent. He/she should have direct access to the board or a board-appointed committee. In case of a separation of duties, the relationship between the chief officers and their respective roles must be clearly defined and well understood.

The chief AML/CFT officer should also have the responsibility for reporting suspicious transactions to senior management, the board, and local Financial Intelligence Unit (FIU). The chief AML/CFT officer should be provided with sufficient resources to execute all responsibilities effectively and play a central and proactive role in the bank's AML/CFT regimen. To do so, he/she must be fully conversant with the bank's AML/CFT regimen, its statutory and regulatory requirements, relevant international standards, and the ML/FT risks arising from the business.

There is an inherent tension between the first-line and the second-line risk management. For example, it is the second line's responsibility to test for compliance or support the quality assurance process to ensure that the first line is meeting internal bank policies, procedures, controls, and risk limits. The inherent risk-based nature of AML/CFT requirements require judgments be made by both the first line and the second line. Compliance and risk choices are not always clear given some unique situations and customer circumstances that create challenges in working through what is the most appropriate decision to meet internal and regulatory requirements. Regardless of a bank's size or its management structure, potential tension between different lines of business can occur and need to be resolved; at times, it may be necessary for issues to be raised to senior management for their view and decision.

THIRD LINE: INTERNAL AUDIT FUNCTION

The internal audit function is responsible for independently assessing the effectiveness of the design and operation of internal controls and compliance practice with laws, rules, and regulations. Internal audit employees independently provide, on an annual basis, a written assessment of their testing of controls and applicable legal compliance. External auditors can also play an important role in evaluating a bank's internal controls and procedures during financial audits, internal control audits, and AML/CFT audits. External auditors can independently confirm a bank's compliance with applicable local regulations and supervisory practices as well as correspondent bank expectations.

The internal audit function plays an important role in the governance and oversight framework through independently and objectively evaluating risk management and controls, and by periodically reporting to the board or a board-appointed committee (that is, an audit committee or a similar oversight body) evaluations of the effectiveness of compliance with AML/CFT policies and procedures. A bank's internal audit program should comprehensively cover

1. *the effectiveness of compliance governance and oversight;*
2. *the adequacy of the bank's policies and procedures in addressing identified risks (including AML/CFT);*
3. *the competence of bank staff in implementing the bank's controls and risk management;*
4. *the detailed testing of critical internal control functions, for example the suspicious activity monitoring and investigations processes; and*
5. *the effectiveness of the bank's training of relevant personnel.*

The board should ensure that audit functions have sufficient resources and appropriate expertise and are knowledgeable of bank operations to conduct such audits. The board should also ensure that the audit scope and methodology are appropriate for the bank's risk profile and that the frequency of such audits and testing is also based on risk. Lastly, internal auditors should formally track and monitor their findings and recommendations for reporting to the board committees responsible for the internal audit process and the lines of businesses.

Summary

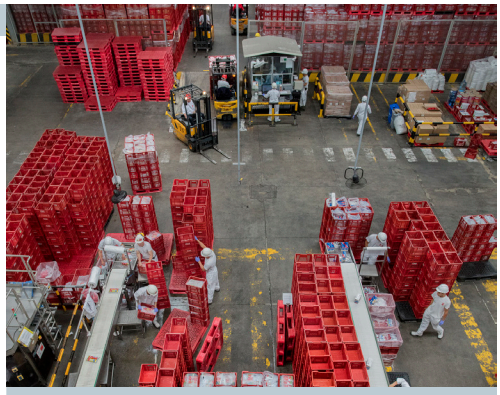
Sound risk management principles apply to the entire spectrum of risks facing a bank. In conducting a comprehensive risk assessment, a bank should consider all the relevant inherent and residual risk factors at the country, sector, bank, and customer relationship levels, to determine the institution's risk profile and appropriate level of mitigation to be applied.

Similarly, banks are required to have a thorough understanding of the inherent ML/FT risks present in its customer base, product offerings, delivery channels, and service offerings (including products under development or to be launched) and the jurisdictions within which it or its customers do business. This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information, such as national risk assessments and country reports from international organizations. Policies and procedures for customer acceptance, due diligence, and ongoing monitoring should be designed and implemented to adequately control the identified inherent risks.[19]

As a key success factor, banks are expected to identify the applicable risks their correspondent relationships pose and implement internal controls to mitigate those risks, including having effective KYC/CDD processes.

[19] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

Chapter 3
Essential Elements of a Sound AML/CFT program



3.1 Introduction

A sound AML/CFT program should be based on a full understanding of the risks faced by the financial institution, relevant regulatory requirements, regulatory guidance, plus the potential impact of noncompliance. An AML/CFT program must incorporate all national requirements and expectations. A bank should also, as business demands, go beyond national requirements to embody global best practices and principles. In addition to this guidance note, the main international AML/CFT standards relevant to emerging-market banks that serve as a starting point include: the FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation; subsequent interpretive notes issued by FATF (together "the FATF 40+9" Recommendations); and BCBS's guidelines on Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

A robust AML/CFT program can reduce the higher perceived risk of respondent banks, thereby improving their standing with a network of large global correspondent banks.

The FATF 40 Recommendations establish a foundational framework of measures that individual countries and banks can build off to effectively manage ML/FT risks. FATF has supplemented its recommendations with interpretive notes and additional guidance documents that address how individuals and businesses can have access to useful and affordable financial products and services that meet their needs delivered in a responsible and sustainable way (financial inclusion[20]) and the risk-based approach,[21] both of which can be helpful in building an effective AML/CFT program. The BCBS guidelines further expand on how banks should manage ML/FT risk based on the FATF 40 Recommendations, which they complement.

Respondent banks should also be aware of major OECD private sector-led industry initiatives intended to clarify ML/FT challenges faced by their partnering correspondent banks. Examples include the best practices and guiding principles for effective ML/FT risk management developed by the Wolfsberg Group,[22] an association of 13 global banks. Their recommended practices are consistent with the other international standards cited.

One helpful initiative undertaken by Wolfsberg is the publication of a model Correspondent Banking Due Diligence Questionnaire[23] used by many OECD correspondent banks to evaluate a respondent bank's AML/CFT practices when considering whether to undertake, maintain, or terminate a CBR. Please note, however that the decision to establish or terminate a CBR is based on more that this due diligence questionnaire. Country risk, ongoing compliance costs, and forecasted revenue are some additional considerations that may outweigh results from a single bank's AML/CFT due diligence. Still, respondent banks may wish to familiarize themselves with this questionnaire and the best-practice standards that are implied when developing their own AML/CFT program

[20] Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (2013)
[21] FATF. Guidance for a Risk-Based Approach. The Banking Sector. 2014
[22] The Wolfsberg Group mission, timeline, and background can be found at https://www.wolfsberg-principles.com/
[23] The Wolfsburg Group Correspondent Banking Due Diligence Questionnaire can be found at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_220218_v1.2.pdf

as this questionnaire is used by many global and large internationally oriented correspondent banks as part of their decision-making process.

Using best AML/CFT risk management practices will enable respondent banks to meet the expectations of correspondent banks that clear and settle offshore transactions in U.S. dollars and euros. This will improve their ability to retain and as necessary obtain new CBRs and to continue providing cross-border banking services to their clients. Beyond maintenance of CBRs, a sound AML/CFT program will minimize the bank's exposure to regulatory sanctions, penalties, and associated reputational risks. As institutions develop more robust AML/CFT programs, ongoing investment can potentially become an operational challenge as resource allocation for AML/CFT compliance typically increases. These additional investments and enhanced AML/CFT controls need to be viewed in terms of the business need to retain, maintain, and obtain a correspondent bank relationship for business purposes and the potential reduction in risks— financial and reputational, for covering sanctions or penalties that may be imposed.

Enhancing AML/CFT programs to ensure continued cross-border banking services are available to clients; your bank remains connected to the global financial system; meets international or other standards; and you ultimately attain a strong, sustainable, and mature compliance program may take several years and be accomplished in stages.

A sound AML/CFT program should include the following interrelated components designed to address all the critical aspects of ML/FT risk management:[24]

1. *Governance*
2. *Risk identification, assessment, and mitigation*
3. *Policies and procedures*
4. *Customer identification and due diligence*
5. *Transaction monitoring*
6. *Reporting*
7. *Communication and training*
8. *Continuous improvement and testing*
9. *Internal and external audit*

The following sections discuss key elements of an AML/CFT program and global best practices to consider implementing to ensure establishment of a robust AML/CFT program to obtain and retain correspondent bank accounts and to provide the offshore banking services demanded by high-value banking customers. In addition, investing in a strong AML/CFT program allows institutions to efficiently and effectively strengthen internal controls, assess risk, and easily respond to any requests related to their AML/CFT compliance program.

3.2 Governance

A sound governance structure is the foundation of an effective AML/CFT program and will include the board of directors and senior management setting the tone at the top, hiring a qualified chief AML/CFT officer, and properly resourcing the three lines of defense. The "tone at the top" is a public commitment at the highest levels of the bank to complying with AML/CFT requirements as part of its core mission and recognition that this is critical to the overall risk management framework of the bank.

The best practices outlined here will strengthen a bank's AML/CFT governance structure:[25,26]

Board of directors	• The board of directors should include people who have a clear understanding of ML/FT risks and who are able to make informed decisions related to AML/CFT matters. The board's awareness of AML/CFT compliance can be increased by training and periodic monitoring of applicable operations. • The board is responsible for approving and overseeing enterprise wide AML/CFT policies and procedures. Depending on the size and complexity of the institution, this responsibility can be carried out by one of the board's committees (for example, the compliance committee or risk committee). • The board should be informed of main compliance risks and plans to mitigate them, at least annually, and be informed of other AML/CFT matters, such as major compliance failures and corrective actions, in a timely and comprehensive manner. • The board should be responsible for appointing a qualified chief AML/CFT officer. The board should continuously monitor the bank's resource allocation to ensure the bank has sufficient expertise, technology, and control systems dedicated to AML/CFT compliance.

[24] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[25] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[26] BCBS. 2015. Guidelines: Corporate Governance Principles for Banks.

Senior management	• Senior management AML/CFT-related responsibilities should include:
	  • Assisting the board in identifying, assessing, and hiring a qualified chief AML/CFT officer;
	  • Communicating and reinforcing the AML/CFT compliance culture established by the board, and implementing and enforcing the board-approved AML/CFT compliance program requirements to ensure compliance with local laws and other policy requirements (for example, any international standards adopted);
	  • Approving and monitoring the AML/CFT risk assessment;
	  • Approving all AML/CFT-related policies;
	  • Approving all major compliance-related initiatives and action plans discussed at the board compliance committee(s), or ad hoc proposals made through the AML/CFT officer;
	  • Monitoring and assessing, through the third line of defense, the effectiveness of established AML/CFT control mechanisms for the bank on an ongoing basis and reporting and escalating to the board areas of concern, as needed;
	  • Ensuring accountability within all lines of defense; and
	  • Incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
	• Senior management should monitor and be informed of critical new AML/CFT compliance risks and weaknesses in the execution of policies, procedures, and risk controls. Corrective action plans should be developed in a timely manner to mitigate issues identified.

First line of defense	• Typically, the business units (for example, customer-facing personnel, front office) are the first line of defense responsible for identifying, assessing and controlling the risk posed by their particular business line or focus. • The business units' personnel should understand and carry out AML/CFT policies and procedures and should be provided with sufficient resources and training to accomplish this part of the organizational mission.
Second line of defense	• The second line of defense includes the AML/CFT compliance function and the chief AML/CFT officer responsible for the execution of specific parts of the AML/CFT compliance (for example, policy and procedure development, operating the suspicious-transaction system, investigation and reporting processes, required currency reporting, and other local law requirements), working closely with the business units to provide training, and an understanding of AML/CFT requirements and risk-based concepts. • They also can perform compliance testing in some areas to ensure that risks in the business units are identified and managed and that policies and procedures are adhered to and in compliance with local laws. **AML/CFT Compliance Function:** • AML/CFT compliance function should have a formal status within a bank and must be independent (for example, compliance personnel should not be in a position where there is conflict of interest between their compliance responsibilities and any other first-line responsibilities they may have). • To employ and retain talent with the required knowledge and skillset, the bank should ensure that the level of compensation is commensurate with the level of expertise and authority. • The compliance function employees should develop key risk indicators (KRIs) to identify, measure, and monitor AML/CFT risks. Detailed reports of KRIs should be made available to all relevant stakeholders from the board of directors and senior management to operational management. • Based on the risk profile of the bank, compliance function employees should design a framework of controls and develop policies and procedures necessary to mitigate the ML/TF risk. • Compliance function employees should have access to all the information and bank personnel necessary to carry out their responsibilities. • Compliance function employees should conduct periodic testing to ensure the first-line internal controls are working as intended. • Compliance activities should be subject to periodic review by independent audit.

	AML/CFT Officer: • The AML/CFT officer should have appropriate qualifications and knowledge of the bank's regulatory requirements and ML/FT risks arising from various lines of business and bank operations. • The officer should be responsible for applicable AML/CFT programs across the entire institution and have sufficient authority and seniority within the bank to be able to influence decisions related to AML/CFT risks and ensure effective fulfillment of AML/CFT requirements by the bank. • If the chief AML/CFT officer reports directly to the chief executive officer (CEO), chief financial officer (CFO), or other senior management, he/she should also report and have direct access to the board. • The officer should report to the board of directors and senior management on AML/CFT compliance matters, including a risk assessment, any changes in the compliance risk profile based on relevant performance indicators, any identified breaches, and the corrective actions. • **Independence of AML/CFT officer is paramount**, and he/she should have the role that is distinct from business-line responsibilities and other executive functions, such as CFO, chief operating officer, or chief auditor. • A bank conducting business nationally and internationally should appoint a chief AML/CFT officer for the entire group. The chief AML/CFT officer should oversee implementation of all strategies and make regular on-site visits to ensure adequate compliance. • The AML/CFT officer should be a point of contact for all AML/CFT-related matters for internal and external parties, including regulators and financial intelligence units (FIUs).

Third line of defense	• The third line of defense is the internal audit function that is responsible for independently assessing the effectiveness of the AML/CFT compliance and risk processes created in the first and second lines of defense.[25] Internal audit employees should have sufficient AML/CFT expertise and auditing experience.
	• Their AML/CFT-related responsibilities should include:
	  • Conducting periodic assessment of relevant AML/CFT program documentation (for example, KYC/CDD/enhanced due diligence [EDD] policies and procedures and procedures related to identifying, investigating, and reporting suspicious transactions);
	  • Conducting testing of AML/CFT controls and processes carried out by both first and second lines of defense, such as KYC/CDD/EDD, training, suspicious-activity reporting, record keeping, and retention, among others;
	  • Conducting periodic evaluation of the bank's AML/CFT risk assessment; and
	  • Following up on any remedial actions arising from independent audit or regulatory findings.
	• Internal audit function employees should be independent and have sufficient authority within the bank to be able to perform their responsibilities with objectivity.
	• Internal audit function employees should report to the audit committee of the board of directors or a similar oversight body.

For effective AML/CFT governance, the board of directors and senior management must demonstrate commitment to their responsibilities in setting the risk and compliance culture at the bank. Effective AML/CFT governance defines and clarifies the responsibilities of all applicable employees and is key to demonstrating the overall effectiveness of the bank's AML/CFT risk management function.

[27] In some emerging market countries, external audit may perform responsibilities related to assessing the effectiveness of the AML/CFT processes created in the first and second lines of defense.

3.3 Risk Identification, Assessment, and Mitigation

Banks must have a thorough understanding of the specific ML/FT risks they face through a periodic enterprise wide AML/CFT risk assessment. Although there are several approaches within the industry to performing an AML/CFT risk assessment, they all commonly include the following three phases:

1. *Identification of inherent ML/FT risks faced by the bank;*
2. *Assessment of internal controls; and*
3. *Assessment of the residual risk, which considers the effectiveness/status of the controls against the inherent risks of the bank. The resulting residual risk should be measured and within the bank's risk appetite.*[28,29]

A robust AML/CFT program can reduce the perceived higher risk of respondent banks, thereby improving their standing with a network of large global correspondent banks.

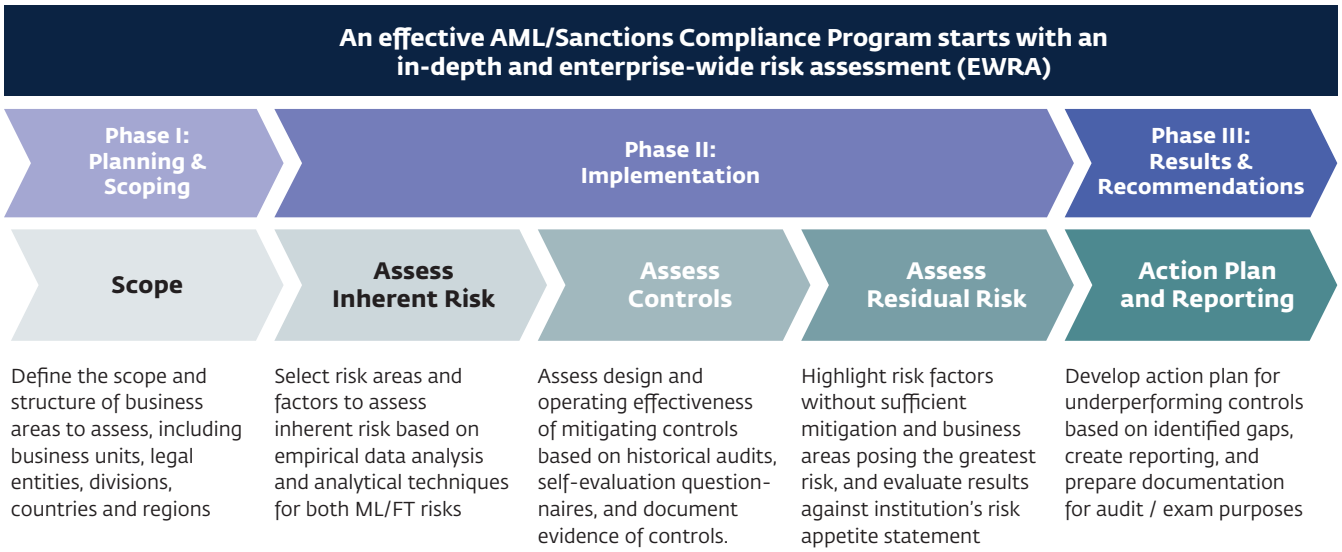
The AML/CFT risk-assessment methodology illustration that appears here is a high-level illustration. A substantial amount of work, data gathering, analysis, and expertise is involved in developing a comprehensive and mature risk-assessment methodology and process. This example should not be interpreted as a one-size-fits-all approach.

PHASE 1: IDENTIFICATION OF INHERENT ML/FT RISKS FACED BY THE BANK

To assess the inherent ML/FT risks faced across all business lines, the bank should include the following risk categories in its risk assessment process:

- *Customer base*
- *Products and services offered*
- *Delivery channels*
- *Jurisdictions*
- *Other qualitative risk factors*

Figure 3: Phases of EWRA



Source: Deloitte Risk and Financial Advisory.

[28] Wolfsberg. 2015. The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption.

[29] The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption (2015) define inherent risk, controls and residual risk as follows: "Inherent Risk represents the exposure to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied." "Controls are programmes, policies or activities put in place by the FI to protect against the materialisation of a ML risk, or to ensure that potential risks are promptly identified. Controls are also used to maintain compliance with regulations governing an organisation's activities." "Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML risks within the FI are being adequately managed."

CUSTOMER BASE

The bank must understand the risks associated with its customers, either individually or as a category. When assessing customer risk, it is essential that the bank establish criteria for identifying high-risk customers. The following factors can be used to differentiate customer risk: customer type, ownership, industry, profession / business, past activities, political / governmental role, product usage, and the customer's transactional activity. Each customer should be risk rated based on the criteria. This information is used by the bank to determine the makeup of its customer base (for example, at a minimum, the percentage of high-risk, medium-risk, and low-risk populations). Banks should consider that certain categories of customers may pose a perceived higher risk. Examples of such customers include:

- *Politically exposed persons (PEPs) (generally have a higher risk of ML/FT when operating in countries characterized by higher levels of bribery and government corruption).*
- *Money or value transfer services providers (considered higher risk as the business is cash intensive and may have poor AML/CFT controls).*
- *Correspondent banking customers (generally considered higher risk when the executing bank must rely on a respondent bank's AML/CFT controls, the strength of which may be unknown).*

PRODUCTS AND SERVICES OFFERED

During the risk-assessment process, a bank should take inventory of the products and services it offers and assess the inherent risk of the products. The assessment should include not only the existing products and services offered by the bank but also those under development or to be launched. Including future product offerings in the assessment helps management forecast if current controls will be sufficient to manage the risk or if additional controls are necessary. Typically, the following products and services have higher ML/FT risk as they have historically been used to place, layer, or integrate the proceeds of crime and thus are considered to have a high ML/TF risk:

- Correspondent banking
- Private banking (domestic and international)
- Trade finance
- Payable through accounts
- Stored-value instruments
- Cross-border, bulk-cash delivery
- Domestic bulk-cash delivery
- International cash letter
- Remote-deposit capture
- Virtual/digital currencies
- Low-price securities
- Hold mail
- Cross-border remittances
- Service to walk-in customers (nonaccount holders)
- Sponsoring private automatic teller machines

In addition to the products listed, wire transfers may present a high degree of risk. Banks should monitor wire transfers and related messages to detect those that do not contain all required beneficiary and/or originator information and to take appropriate measures to prevent processing of wire payments associated with designated persons and entities (for example, persons and entities subject to financial restrictions because of human rights abuses, terrorist activity, or other reasons). Complete and accurate records are critical to AML/CFT risk management and to demonstrating compliance because transparency is essential in managing these risks and protecting the bank from possible criminal abuse.

DELIVERY CHANNELS

The risk assessment should also consider delivery channels. Certain delivery channels (for example, business relationships or transactions that are not face to face) may pose a higher ML/FT risk as they increase the challenge of verifying the customer's identity and activities.

JURISDICTIONS

The risk assessment must consider the risks associated with jurisdictions in which the bank operates as well as the risk associated with jurisdictions in which the bank's customers conduct business. A bank should conduct the analysis to understand its geographic footprint and determine the number of customers within each country. Determining the number of customers in different jurisdictions can be based on either some or all of the following factors: domicile, nationality, and/or incorporation. When assessing jurisdiction risk, the bank can use an externally purchased country risk methodology/model or develop its own for sub-national jurisdictions that pose higher risk. If a bank

undertakes the development of its own methodology, it should consider leveraging country reports from international organizations that identify countries subject to economic sanctions, known to be supporting international terrorism, and those with deficiencies in combatting money laundering and terrorist financing, such as a list of high-risk and other monitored jurisdictions published by FATF[30] or the OECD Country Risk Classification.[31] In addition, the Basel AML Index[32] is an independent annual ranking that assesses the risk of ML/TF around the world.

OTHER QUALITATIVE FACTORS

There are other qualitative factors that can affect the bank's inherent risk and therefore should be or may be considered during the ML/FT risk assessment. Some of the qualitative factors that should be considered are:

- *Expected account and revenue growth;*
- *Recent AML/CFT compliance personnel turnover;*
- *Reliance on third-party providers to perform AML/CFT program requirements and responsibilities;*
- *Recent enforcement actions and/or penalties; and*
- *Independent audit and regulatory findings.*

The figure below provides a summary of the assessment of inherent risks. The listed risk factors and measures are for illustrative purposes only and should not be viewed as exhaustive.

PHASE 2: ASSESSMENT OF INTERNAL CONTROLS

After a bank identifies its inherent risks, the second phase of the process involves assessing the quality of existing controls to determine how well they manage the identified risks. The bank is to evaluate the overall design and operating effectiveness of existing controls. Control effectiveness can be assessed through a self-assessment and challenges by subject matter experts. Independent audit testing and internal compliance testing results should also be considered in determining the effectiveness of internal controls.

The following illustration shows an AML/CFT controls assessment approach. This methodology is commonly used for the control portion of the risk-assessment process and involves the creation of control questionnaires (see "sample control categories") to assess and document the status of each of the critical controls. The results of the controls assessments and subsequent calculation of the effectiveness of the controls are then compiled and summarized through various risk levels (see "satisfactory," "needs improvement," and "unsatisfactory" ratings). This phase of the risk-assessment process also requires a substantial amount of

Figure 4: Risk Factors

Example Inherent Risk Factors and Measures:

RISK FACTORS	Customer Base	Products/ Services	Delivery Channels	Jurisdictions	Qualitative Factors
ILLUSTRATIVE MEASURES	• Legal form/ ownership structure • Length of relationship • PEP status • Industry • Customer Risk Rating (CRR)	• High degree of anonymity or limited transparency • Rapid movement of funds • High volume of currency or equivalents • Payments to/ from third parties	• Account origination • Account servicing	• Location of business • Location of clients • Origin or destination of transactions	• Growth vs. stability • Mergers & acquisition • Strategy changes • New regulatory requirements • Emerging risks

Source: Deloitte Risk and Financial Advisory.

[30] http://www.fatf-gafi.org/countries/#high-risk
[31] http://www.oecd.org/trade/xcred/crc.htm
[32] https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf

work, control assessment creation, data gathering, analysis, and expertise to develop a comprehensive and mature control risk-assessment methodology and process.

Risk identification and assessment should be based on internal information, such as operational and transactional data produced by the bank, as well as external information, such as country reports from various international organizations and national risk assessments. The risk-assessment methodology should include both quantitative and qualitative elements (for example, volume and value of transactions)[33] and be clearly documented and approved by senior management.

PHASE 3: ASSESSMENT OF RESIDUAL RISK

Once a bank has assessed its inherent risks and the effectiveness of controls designed to mitigate, phase three of the risk assessment can be completed. The residual risk is the remaining risk after controls are applied to the inherent risk. It is a process by which the aggregated conclusions are deduced from both the inherent and controls risk assessment and a residual risk determination is made (see the following residual risk approach illustration). The residual risk indicates whether ML/FT risks posed by the bank are being effectively managed. For example, if the bank's inherent risks are considered "medium" and the controls are rated "unsatisfactory," based on the three-tier scale[34], the residual risk rating would be "high." As illustrated in Figure 6, this "high" residual risk rating is found at the intersection of the "medium" risk rating and the "unsatisfactory" control rating.

The frequency of the risk assessment varies depending on a number of factors, such as the domestic regulatory requirements, mergers and acquisitions affecting the risk profile of the bank, new products and services, results of the risk assessment, and potentially correspondent bank expectations, as well as others.[35] It is common for banks to perform risk assessments annually. However, banks should update their risk assessment more frequently than annually if they identify new or emerging risks that significantly change the bank's risk profile (for example, when expanding to new markets or geographies or implementing new delivery channels).

Although banks can rely on external parties or externally purchased technology to conduct risk assessments, they should remember that the responsibility for assessing and managing risk ultimately lies with the bank board and senior management and cannot be "outsourced." If the bank engages an external party to assess risk, the external party must follow the risk-assessment methodology and relevant policies and procedures established by the bank and local requirements. In case of an externally purchased technology/risk assessment model, the bank should take

Figure 5: Risk Control Categories

Sample Control Categories:

- AML/CFT Corporate Governance, Management Oversight and Accountability
- Policies and Procedures
- Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Simplified Due Diligence (SDD) and Politically Exposed Persons (PEPs)
- Previous Other Risk Assessments
- Management Information System (MIS) / Reporting
- Record Keeping and Retention
- Designated AML/CFT Officer
- Detection and Suspicious Activity Report (SAR) Filing
- Monitoring and Controls
- Training
- Independent Testing and Oversight
- Other Controls

Illustrative Risk Levels:

91-100% **Satisfactory:** Substantially meeting all control requirements

75-90% **Needs Improvement:** Meeting between 75% and 90% of control requirements

<75% **Unsatisfactory:** Meeting less than 75% control requirements

Source: Deloitte Risk and Financial Advisory.

[33] BCBS. 2015. Guidelines: Corporate Governance Principles for Banks.
[34] This illustration is of a three-tier rating scale. Some institutions use four-tier rating scales, which include the following ratings for "inherent" risk: high, medium-high, medium, and low and the following ratings for "controls" assessment: strong, satisfactory, needs improvement, and unsatisfactory. Residual risk determination ratings include: high, medium-high, medium, and low.
[35] The Wolfsberg Group's Correspondent Banking Due Diligence Questionnaire suggests that the frequency of the enterprise wide risk assessment should be 12 months.

Figure 6: Residual Risk

Illustrative Residual Risk Approach:

- Residual risk is determined by balancing the inherent risk with the overall strength of the risk management activities/controls
- The residual risk rating is used to assess whether the ML/FT risks within the business unit as well as for the institution as a whole are being adequately managed
- The residual risks should be calculated across each business unit
- The residual risks should be available in a visual heatmap format

Illustrative Residual Risk Matrix:

Residual Risk Determination		Inherent Risk		
		Low	Medium	High
Control Assessment	91 – 100% Satisfactory	Low	Low	Medium
	75 – 90% Needs Improvement	Low	Medium	High
	<75% Unsatisfactory	Medium	High	High

Source: Deloitte Risk and Financial Advisory.

necessary steps to validate the technology and ensure it addresses the needs of the bank.[36]

The results of the risk assessment, the methodology employed, and any measures taken by the bank to manage the identified risks should be consolidated within a comprehensive report and communicated to the board of directors and senior management in a timely, complete, and accurate manner. This will help not only the board but also senior management, the CRO, and the chief AML officer in making informed decisions and ensuring that the bank's resources, expertise, and technology are aligned with mitigating its risks.

[36] BCBS. 2015. Guidelines: Corporate Governance Principles for Banks.

Example: Risk Assessment

Inherent Risk Assessment:

The assessment of inherent risk can be conducted by administering questionnaires for qualitative risk factors and by extracting quantitative data from the relevant bank systems. A bank should be prudent about the threshold for the quantitative risk factors based on its risk appetite and provide risk weights to both the qualitative and quantitative factors.

The information gathered should be populated against the ML/TF inherent risk-assessment questionnaire to calculate the bank's inherent risk. The ML/TF inherent risk-assessment questionnaire should cover critical areas of the bank's business (for example, customers, geographies, products, services, transactions, and delivery channels) and consider the operational and regulatory risk factors that should be taken into account when assessing the robustness of the AML/CFT program (for example, introduction of new products, expansion into new markets, mergers and acquisitions, new regulatory requirements, recent regulatory actions, and so forth).

Mitigating Controls Assessment:

To assess the mitigating controls, the bank should create a register of regulatory requirements or obligations, including known regulatory expectations and applicable industry-leading practices (with respect to known ML red flags and typologies). The bank's policies and procedures and process controls that have been implemented should be mapped against the register. This exercise should lead to identification of control gaps, if any.

The controls that are implemented should be tested for effectiveness. Its strongly recommended that banks consider the following while assessing control effectiveness:

1. Review of the bank's policies and procedures to identify any gaps between the policies and regulatory requirements;
2. Walkthroughs with the business and operations teams to identify if the policies and procedures are being operationalized effectively (that is, implemented and operating as designed); and
3. Sample testing against key control indicators and control sample testing thresholds.

The controls in place should be periodically reviewed and tested for effectiveness and whether any change in the inherent risk of the business or residual risk necessitates enhancement of such controls.

Source: Adopted from "Best Practices for Countering Trade Based Money Laundering" 18 May 2018 published by AML/CFT Industry Partnership (ACIP) https://abs.org.sg/industry-guidelines/aml-cft-industry-partnership.

3.4 Policies and Procedures

AML/CFT policies, procedures, and internal controls should be designed to mitigate the inherent risks identified by the risk assessment. They should address the unique risks and bank risk profile. AML/CFT policies and procedures should be in writing and serve the purpose of preventing, detecting, and reporting potentially suspicious activity, complying with local laws, and establishing a strong internal control and risk management environment.

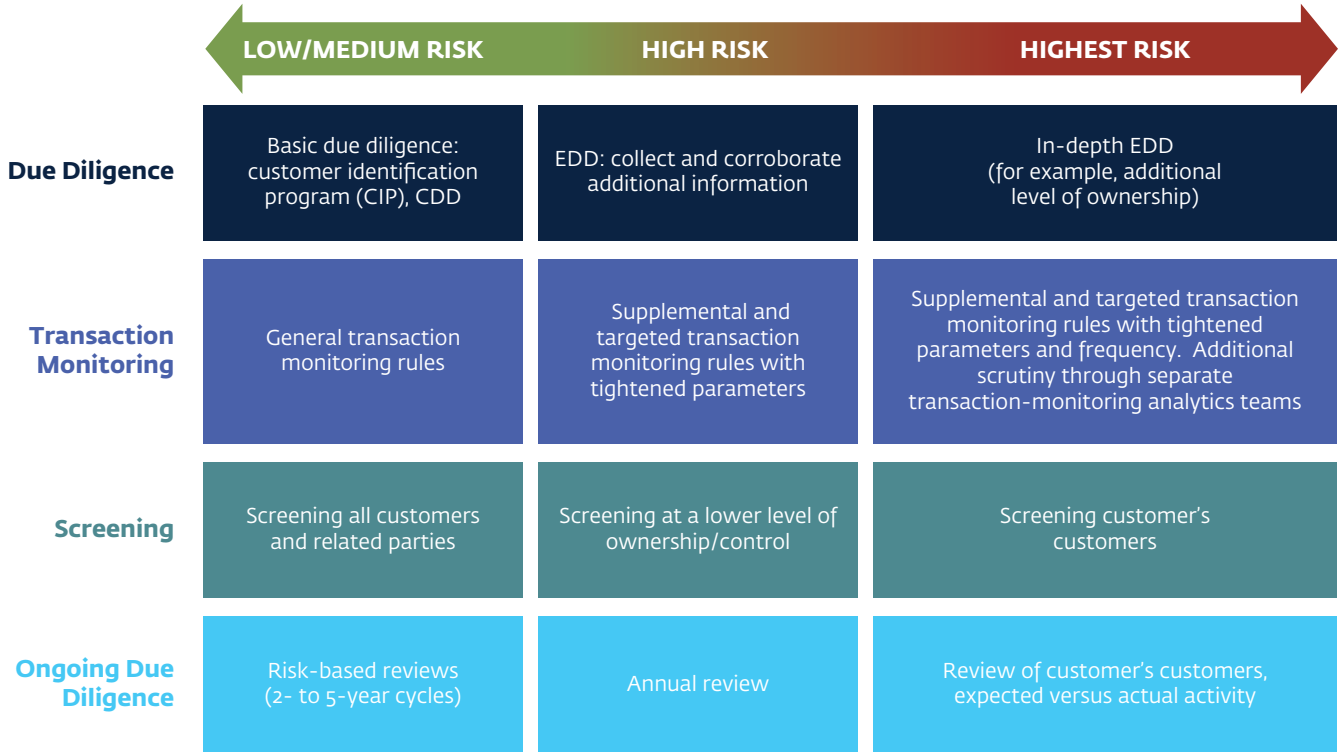
When designing and implementing policies, procedures, and internal controls, the bank should use a risk-based approach. This approach implies that higher-risk customers, higher risk products, or other factors may necessitate more stringent controls and ongoing monitoring. The following is an illustrative example of a risk-based approach for policies and procedures and other AML/CFT controls.

AML/CFT policies and procedures should[37,38]

[37] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[38] The Wolfsberg Group. 2018. Correspondent Banking Due Diligence Questionnaire.

Figure 7: Applying a Risk-Based Approach

Activities Driven by Customer Risk Levels – For Illustrative Purposes Only



Source: Deloitte Risk and Financial Advisory.

- *Be approved by the bank's board or directors or senior committee.*
- *Designate a chief AML/CFT officer to coordinate and oversee the AML/CFT program.*
- *Outline processes regarding the assessment of the AML/CFT program by either an internal audit or independent third party.*
- *Document the processes regarding AML/CFT training; policy updates; CDD and EDD; due diligence conducted on or by other banks; detecting and reporting potentially suspicious transactions; reporting of currency transactions; responding to law enforcement requests; and sanctions compliance.*
- *Use a risk-based approach to apply CDD standards to all new accounts, as well as refresh CDD on existing relationships as necessary.*
- *Outline processes regarding screening for PEPs.*
- *Document a retention policy in which banks maintain all necessary records; records should be kept for 5 years or the time period complying with local law.*
- *Be consistent throughout the organization, with adjustments made in accordance to the risk of the business line or geographic location of the operation.*
- *Be applied to all branches and subsidiaries in the home country, as well as in locations outside of the jurisdiction (if applicable).*
- *Be updated on a regular basis and disseminated and accessible to all relevant personnel.*

AML/CFT policies and procedures should not[39,40]

- *Allow anonymous accounts or accounts in obviously fictitious names.*
- *Allow correspondent banking relationships with shell banks.*
- *Allow transactions with designated persons and entities.*
- *Be a "cut-and-paste" guide from documentation found on the Internet or another institution's procedures.*
- *Be outdated and provide inconsistent information.*

[39] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[40] FATF. 2018. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

AML/CFT in a Groupwide and Cross-Border Context

Financial institutions operating in multiple jurisdictions should consider developing groupwide AML/CFT policies and procedures to ensure that they are accounting for risk across their international operations. Policies and procedures at the branch or subsidiary levels should not only reflect local requirements and considerations of the host jurisdiction but also be consistent with and support groupwide policies and procedures.

If legal requirements differ between the home and host countries, the higher standard of the two should be followed. Additionally, if a jurisdiction does not allow for the proper implementation of standards, the chief AML/CFT officer should inform the home supervisors.

Another important consideration for banks with international operations is the extent to which the bank can rely on procedures from other banks when business is being referred. Banks must ensure that they do not allow for policies and procedures that are less strict than their own, meaning that banks must do their own due diligence on the standards used in the jurisdiction of the referring bank. If the introducer is part of the same financial group, a bank could rely more heavily on the introducer's customer information, so long as the introducer abides by the same standards as the bank and the application of the standards is supervised. If a bank takes this approach, it should still obtain customer information (KYC and transaction data) from the referring bank in case the referred customer is found to be engaging in suspicious activity.

If implementing centralized systems and databases, a bank should have adequate documentation of all local and centralized functions to ensure monitoring of suspicious activity across the entire group.

To ensure that the groupwide ability to obtain and review information regarding the groups' global AML/CFT standards is met, vigorous information sharing among the head office and all branches and subsidiaries (when allowed) must be encouraged. A bank's groupwide policies and procedures should include a process, to be followed in all jurisdictions, for identifying, monitoring, and investigating potentially suspicious activity; this includes the coordination of information sharing when necessary. Branches and subsidiaries should be able to provide the head office with information relating to high-risk customers and specific activities that are considered relevant to the global standards. All requests made by the head office should be answered in a timely manner.

When designing policies and procedures regarding information sharing requests, the bank should consider:

- Any local laws and regulations related to data protection and privacy of customers.
- How to handle requests from law enforcement, supervisory authorities, or FIUs.
- The type of information that can be shared and requirements for storage, retrieval, distribution, and disposal.
- The potential risks posed by the reported activity, the risk of a given customer or group of customers, and if other branches or subsidiaries also hold accounts for that customer.

Source: Excerpt from BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

3.5 Customer Identification and Due Diligence

To manage ML/FT risks effectively, banks must understand who their customers are. To achieve this, banks must conduct customer identification and due diligence when onboarding a new customer, as well as update CDD throughout the banking relationship with the customer. The following tables outline when banks should be required by regulators to conduct CDD, when partner correspondent banks will be expecting vigorous CDD, and what CDD measures they must be undertaking:

When should banks perform CDD?

Financial institutions should be required to conduct CDD when:

- Establishing a new business relationship.
- Carrying out occasional transactions (i) above the applicable designated threshold (equivalent to $15,000/€ 15,000) or (ii) that are cross-border and domestic wire transfers
- There is suspicion of money laundering or terrorist financing.
- The financial institution has doubts about the veracity or adequacy of the previously obtained customer identification data.

If the financial institution is unable to comply with these requirements, it should be required to:

- Not open the account, commence business relations, or perform the transaction.
- Terminate the business relationship.
- Consider filing a suspicious-transaction report in relation to the customer.

Source: Excerpt from FATF Recommendation No. 10.

What CDD measures should banks undertake?

Financial institutions should be required to conduct the following CDD measures:

a. Identifying the customer and verifying the customer's identity using reliable, independent source documents, data, or information.
b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner.
c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and the customer's business and risk profile, including where necessary, the source of funds.

Source: Excerpt from FATF Recommendation No. 10.

Banks are to apply each of these CDD measures to all customers; however, these measures or additional measures should be determined based on a customer risk level. When assessing customer risk, a bank should consider relevant factors, such as the customer's background (for example, occupation), country of origin or residence, bank products used, nature and purpose of account, transactions, and business activities.[41]

CUSTOMER RISK RATING PROCESS

Customer risk ratings support the bank's decision whether to enter, continue, or terminate the business relationship and determine the level of controls needed to be employed to manage the risk, including the type of ongoing suspicious-activity monitoring. Customer risk ratings and profiles can be developed at either the individual customer level or for groups of customers displaying similar characteristics (for example, a group of retail customers who have a similar income range and conduct similar transactions).[42] The following figure is a summary of a CRR process that

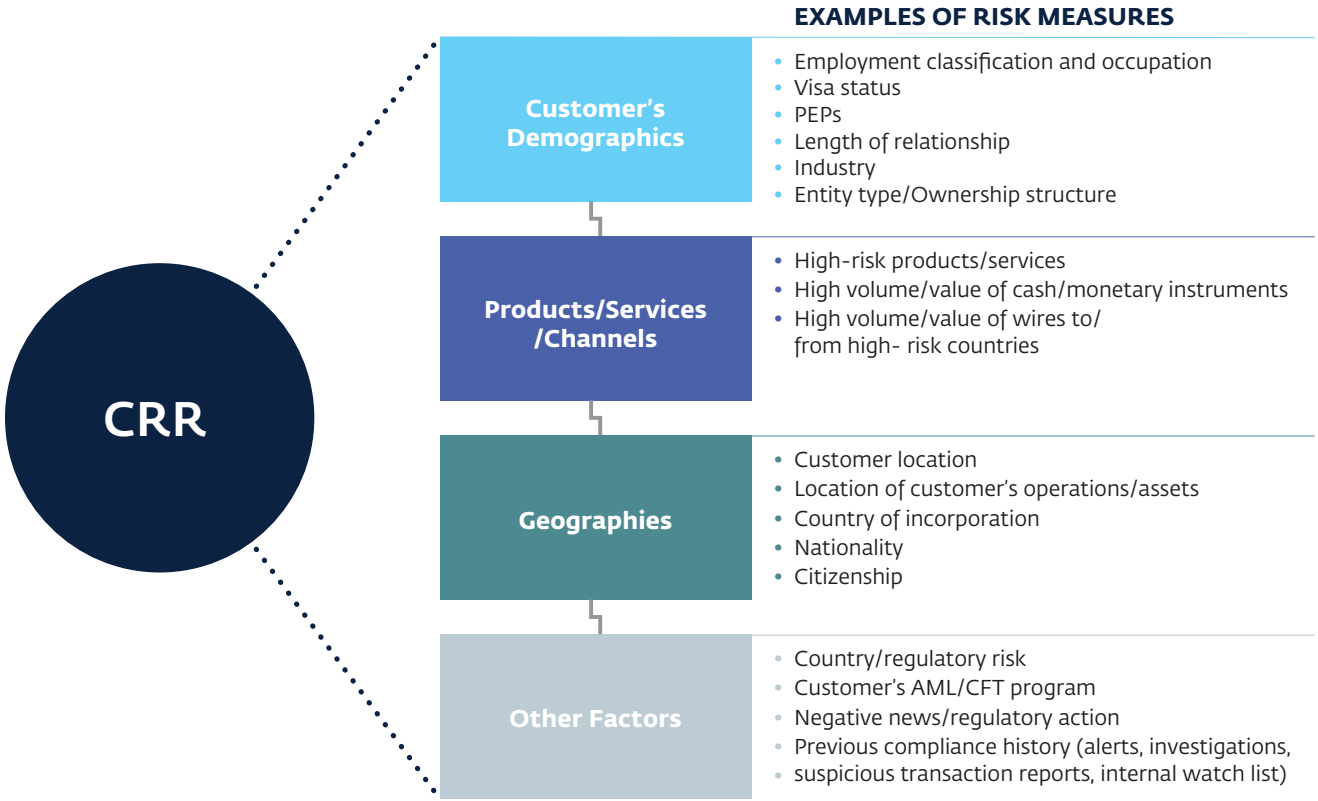
[41] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[42] FATF. 2014. Guidance For a Risk-Based Approach. The Banking Sector.

presents and takes into account various risk measures. Similar to the risk-assessment process, the CRR process requires a substantial amount of work, data gathering, analysis, and expertise to develop a comprehensive CRR methodology and process.

For customers deemed to be of a lower risk, simplified due diligence measures may be allowable. If the customer risk is deemed to be higher, enhanced controls and CDD/EDD measures should be taken by the bank to mitigate risk.

The bank should also develop clear customer acceptance policies that lay out circumstances under which a new relationship would not be accepted, or a current relationship would be terminated. When implementing a customer acceptance policy, it is important that it not be so restrictive that it results in the denial of customers who are considered financially or socially disadvantaged; a risk-based approach should be taken to understand and mitigate risk as opposed to simply avoiding it.[43]

Figure 8: Customer Risk Rating (For Illustrative Purposes Only)



Source: Deloitte Risk and Financial Advisory.

Lower-Risk Customer Examples	Higher-Risk Customer Examples
• Low transaction volume retail customers • remittance customers are ONLY low risk if there are low amounts of transactions and and low aggregate annual volumes • Publicly held companies traded on a recognized stock exchange filing quarterly financial reports and annual audited financial statements. • Financial institutions on a recognized stock exchange in a compliant country (Note: depending on other factors, such as transactional activity and geographies, the customers listed above can present higher risk.)	• High net worth individuals • PEPs • Government entities of a high-risk country • Money transfer operators (MTOs) • Automatic teller machine operators • Casinos • Foreign private investment corporations • Trusts and shell companies in offshore jurisdictions

[43] FSD Africa. 2017. Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism

Examples of Enhanced Due Diligence/Simplified Due Diligence measures

Enhanced Due Diligence (EDD)

- Obtaining additional information on the customer (for example, occupation, volume of assets), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

Simplified Due Diligence

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (for example, if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of ongoing monitoring and scrutinizing transactions based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

Source: Excerpt from FATF. 2018. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

When developing their customer acceptance and customer due diligence policies and procedures, banks should give special consideration to the treatment of PEPs (whether as customer or beneficial owner). In relation to foreign PEPs,[44] besides performing normal customer due diligence, banks should:[45]

- *Have appropriate systems to determine whether the customer or the beneficial owner of a legal entity is a PEP;*
- *Obtain senior management approval for establishing or continuing such relationships;*
- *Take reasonable measures to establish the source of wealth and source of funds; and*
- *Conduct enhanced ongoing monitoring of such relationships.*

Banks should also take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases in which such PEPs present higher risk, banks should apply the same requirements to them as for foreign PEPs.[46]

To adequately assess the risks posed by PEPs, banks should consider obtaining and evaluating the following information:

[44] The FATF Recommendations define PEPs as follows: "Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.
The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories."

[45] FATF. 2018. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

[46] FATF. 2018. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

- *The position the PEP holds/held;*
- *Whether this position is/was in a higher-risk country;*
- *Whether the PEP has the ability to move government funds;*
- *Nature of the PEP's current business;*
- *Pattern of related transactions;*
- *The PEP's source of wealth and source of funds; and*
- *The PEP's reputation.*

Banks' policies and procedures should clearly outline what additional due diligence is required for PEPs. The requirements for PEPs should also apply to family members or close associates of such PEPs.

As noted, when conducting due diligence, the bank should take reasonable measures to identify and verify the identity of beneficial owners (when the customer is a legal entity). This includes knowing and understanding the ownership and control structure of the customer and determining whether the beneficial owner is a PEP (whether foreign, or domestic, or a person who holds a prominent position by an international organization), a designated person, or an individual associated with negative news. If requested by law enforcement or other authorities, information on all beneficial owners and controls should be given in a timely manner.

Banks should be able to demonstrate that they truly know who their customers are. For example, if the bank determines that 20% of a corporate customer is owned by a trust, the bank's due diligence efforts should not stop there. The bank should gather sufficient information about the trust itself and any related parties, such as the settlor, trustee(s), and beneficiaries.

Due diligence should be applied not only to customers and beneficial owners but also to persons acting on behalf of the customer. The bank should ensure that any individuals acting on behalf of the customer are authorized to do so and should verify the identity of such individuals.

To verify the identity of a customer, beneficial owners, or authorized persons, the bank should use reliable, independent source documents, data, and information. If using supplemental sources other than official documents, banks should ensure that the methods and sources are in line with their jurisdictional requirements and expectations and the bank's policies and procedures. These methods may include obtaining financial statements or checking references with other banks and recognized entities such as public utilities.

The nature and extent of the information required for verification will depend on the customer risk rating and risk assessment conducted by the bank on the customer.

For large integrated or cross border financial groups incorporating numerous financial institutions, there should be shared CDD policies and procedures. However, based on the risks inherent in each sector of business, CDD measures should be tailored for each specific group.

For additional information on collection of customer information and verification of customer identity, please refer to Annex 5, which has specifics and details covering this subject.

Banks should ensure that the information collected as part of CDD is kept up to date by developing policies and procedures regarding the frequency of confirming and collecting customers' CDD. Review of higher-risk customers should be performed more frequently and should require enhanced due diligence. It should be noted that terrorist and sanctions screening should be performed on all customers, irrespective of the customer risk profile. Banks should consider using automated solutions to conduct such screening and should freeze without delay and prior notice the funds/assets of identified designated persons and entities, as required by applicable laws.

The bank should conduct periodic screening of its customer base to identify high-risk customers requiring EDD (for example, PEPs) or any prohibited customers (for example, designated persons and entities).

CDD and the related customer risk ratings optimally should be held in a centralized database or in a system that provides access to anti-money laundering and sanctions compliance officials responsible for bank compliance. Management information systems (MISs) provide key information about customers and their activities to both business units and compliance personnel. MISs should be able to provide all necessary information about the customer, such as account documentation, transactional history, and any changes in the customer profile; this information should be provided at the enterprise wide level (across all business lines).

Ongoing Monitoring – For Illustrative Purposes Only		
Risk Level	**Frequency**	**Illustrative Steps to be Taken by the Bank**
High risk	Every 12 months	In relation to customers who did not trigger an alert, the bank may consider refreshing required information by sending an automated e-mail asking the customer to confirm baseline information on file. For customers who triggered an alert, a more in-depth assessment, including a manual request for information (RFI) and review of the customer activity, may be required.
Medium risk	Every 18–36 months or trigger-based reviews	
Low risk	Every 36–60 months (for corporate customers) Trigger-based reviews (for retail customers)	

RELIANCE ON THIRD PARTIES

CDD compliance is ultimately the responsibility of the bank. There may be times, however, when a bank is permitted to rely on third parties to perform certain elements of the CDD procedures. Allowing a third party to conduct CDD must be permissible based on local laws. A bank must ensure that it is within legal boundaries to outsource the collection and updating of CDD. Banks should verify that their jurisdiction privacy laws permit these types of activities. A bank may use a third party for[47]:

- *Identifying and verifying the customer's identity using reliable, independent source documents, data, or information.*
- *Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner. For legal persons, this should include understanding the ownership and control structure of the business.*
- *Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.*

When using a third party, the following minimum criteria must be met:

- *The bank must receive the CDD information collected on the customer before onboarding.*
- *The bank should take adequate steps to ensure that all documentation, including copies of identification data, are received or available to them without delay from the third party.*
- *The bank should satisfy itself that the third party is regulated, supervised, or monitored appropriately and has measures in place for CDD and record-keeping compliance.*

EMERGING TECHNOLOGY SUPPORTING KYC/CDD

There are a number of emerging technology applications that have the potential to improve the efficiency and effectiveness of AML/CFT processes and thereby improve a bank's operations. Several global banks are experimenting with multiple technologies that address some AML/CFT compliance challenges.[48] Smaller institutions may also benefit from the new technologies in terms of compliance and cost saving and in terms of obtaining and maintaining CBRs. Some of these innovations are described here.

KYC UTILITIES

KYC utilities may take several forms as described in the text box below. Focusing on one type, the use of KYC utilities that take the form of a centralized database registry is an innovative way for banks to store collected CDD information. KYC utilities can help a bank's procedures by reducing the amount of data redundantly sent from respondent banks to correspondent banks. Utilities also allow correspondent banks to monitor their respondent banks on an ongoing basis. There are three common challenges correspondent banks and their respondent banks face when it comes to KYC document collection without use of a utility:

1. *Typically, the same, or similar, information needs to be collected by all correspondents making use of the widely popular Wolfsberg Group Correspondent Bank Due Diligence Questionnaire.*
2. *Some correspondents have differing KYC due diligence requirements.*
3. *The KYC due diligence collection and ongoing monitoring process is labor intensive and can be complex, costly, and time consuming.*

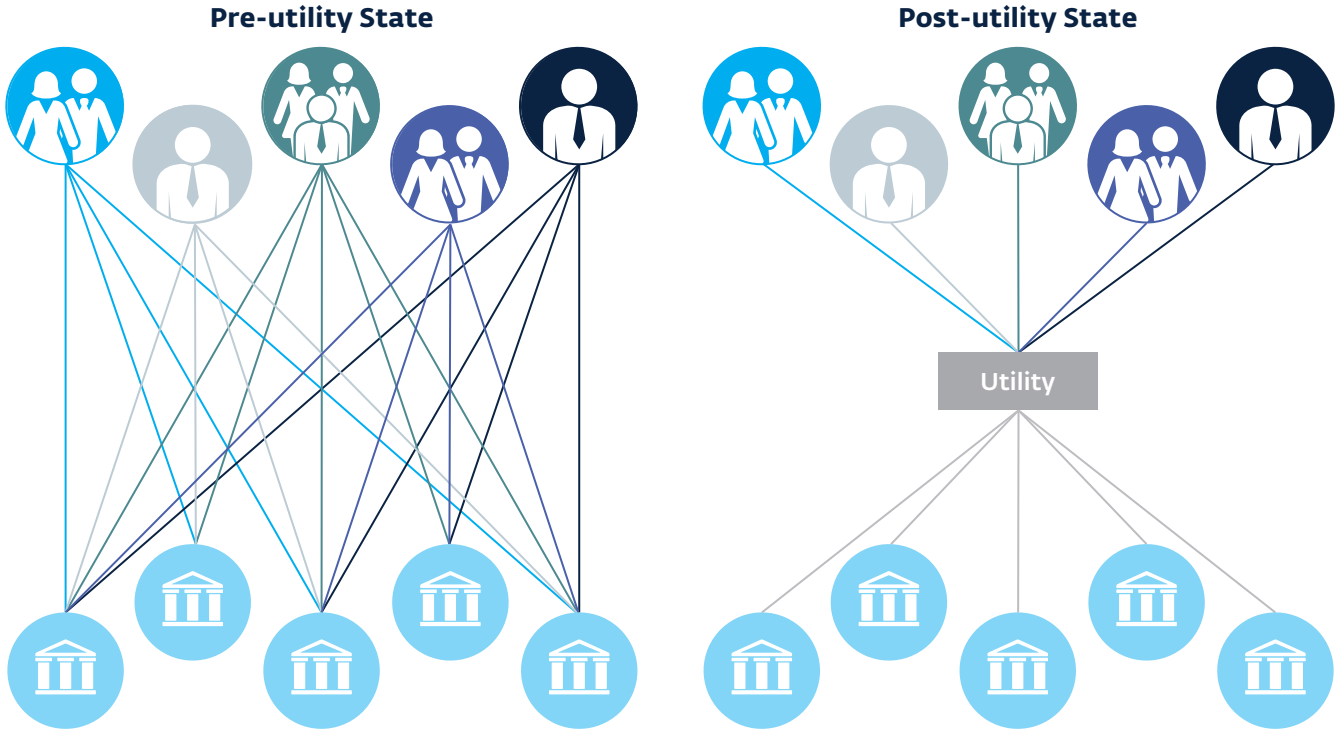
[47] FATF. Feb 2018. FATF Recommendations
[48] IFC. 2018. A Guide to Respondent Banks: Essential KYC Considerations to Manage Correspondent Banking Relationships in Trade.

Figure 9 illustrates how KYC utilities can centralize KYC activities and assist with the aforementioned problems.

There are a number of advantages that KYC utilities provide, including:

1. *Respondent banks enter applicable KYC due diligence into one database for all correspondent relationships to access and use. This greatly reduces the number of times the respondent needs to collect and send similar information to their various correspondent banks.*
2. *Correspondent bank transactional costs may be reduced thanks to a need to provide, update, and exchange KYC due diligence documentation with only one entity, the KYC utility.*
3. *The use of a single template promotes the standardization of the KYC due diligence information collection, which typically covers most of the correspondent banks' KYC obligations.*
4. *The use of a KYC utility greatly reduces the amount of additional unique KYC due diligence of each correspondent bank.*
5. *The accuracy and consistency of the KYC due diligence information is improved because respondent banks maintain only one set of updated information within the utility.*
6. *The use of a centralized KYC utility speeds up the availability of KYC due diligence information for correspondent banks when they are considering starting a relationship or opening an account with a respondent bank.*[49]

Figure 9: Centralizing KYC Activities



Source: IFC. May 2018. A Guide to Respondent Banks: Essential KYC Considerations to Manage Correspondent Banking Relationships in Trade.

[49] CPMI. 2016. Correspondent Banking.

FRESH IDEAS ABOUT EMCompass BUSINESS IN EMERGING MARKETS

www.ifc.org/thoughtleadership NOTE 59 • OCT 2018

What is a Know-Your-Customer Utility?

There are three types of KYC utilities operating today: **Industry Collaboration Utilities, Jurisdictional Utilities**, and **Utility Service Providers**. Two subcategories of utility service providers are: a) Utility Services, which are primarily data services and identification (ID) information storage; and b) **Managed Services**, which are basically outsourced utility services, plus transaction tracking and CDD. Examples of each type of utility are as follows:

Industry Collaboration Utility: SWIFT

CDD requires records of where customer payments originate and terminate. This explains why one of the first successful KYC utilities was introduced by SWIFT, the Society for Worldwide Interbank Financial Telecommunications.

Essentially, SWIFT deals in electronic messages between banks, and these messages provide a transaction trail, documenting where money originates and terminates. SWIFT does not clear or settle transactions, and holds no accounts, but does pass information about payments through its highly secure messaging system. SWIFT has a successful shared data repository that holds profile data for hundreds of respondent and correspondent banks. The SWIFT KYC utility, available to SWIFT members, is useful for member correspondent/respondent banking relationships, and reduces correspondents' risk when dealing with respondent banks in high-risk or sanctioned jurisdictions because the SWIFT utility validates where the money goes, and that the recipient is acceptable. The utility, which is used by major correspondent and respondent banks, is used primarily for the larger payments of larger corporations. There are around 11,000 SWIFT users today, which makes SWIFT a significant player in international corporate payments; however, many smaller banks and FIs in emerging markets are not SWIFT members.

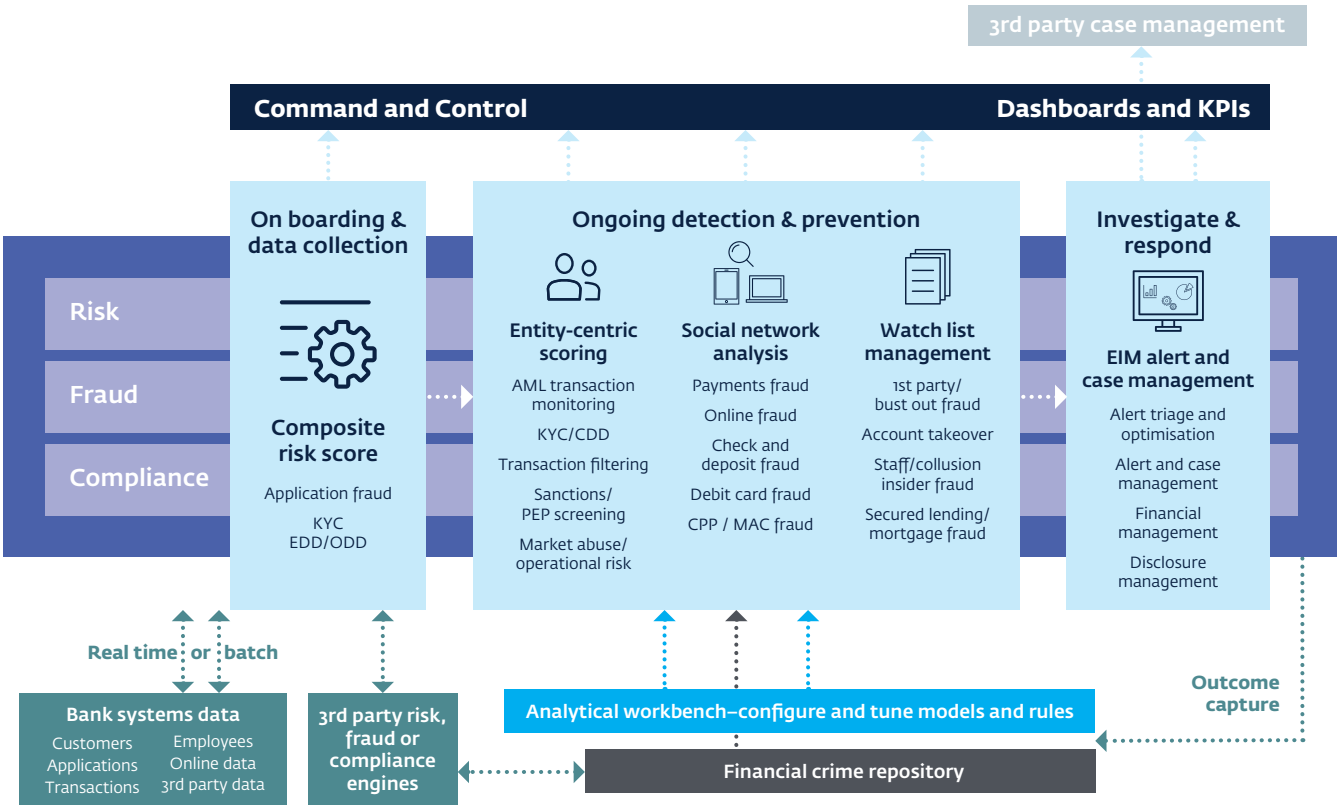
Jurisdictional Utility: Monetary Authority of Singapore KYC Utility

In 2017 the Monetary Authority of Singapore announced development of a national KYC utility that would cover all individuals with accounts in Singapore. The "MyInfo" service, a personal data platform that contains government verified personal details for every account holder, is the foundation for this utility. Residents provide their data to the government once, and it then supports all subsequent online transactions. The goal is to link all FIs to this validated database, which will reduce redundancy and improve information quality. Singapore has the advantage of a very good national ID system and database, and the nation is highly digitally enabled. Its utility does not address transaction monitoring or ongoing CDD; that role is retained by the individual FIs. A more ambitious effort by MAS to do the same for corporate banking transactions was recently put on hold in November 2018 pending a review of implementation costs and anticipated savings.

Utility Service Provider: BAE Systems

BAE Systems is the largest defense contractor in the world and offers its "NetReveal" product as a managed service for KYC/CDD solutions. This enterprisewide approach is intended to satisfy all KYC/CDD requirements for the financial institutions (primarily European banks) that outsource financial functions to BAE. BAE's system includes customer information capture, validation, risk rating, politically exposed person (PEP) checking, investigation, regulatory reporting, continuous monitoring, beneficial ownership validation, risk ratings, changes in management, adverse events, business expansion, new lines of business, initial public offerings (IPOs), acquisitions, divestitures, geographic expansion, social media coverage, credit rating changes, etc. The system also monitors transactions and uses artificial intelligence (AI) and other applications to automate most of these activities (**Figure 10**). *(continued on next page)*

Figure 10: BAE's KYC Utility Product Offering—The NetReveal risk, fraud, and compliance solution suite



Source: www.baesystems.com

To be ready to use KYC utilities, a bank must have the internal capacity and infrastructure to enter and update all essential data regularly. This may require a significant technology investment on the part of the bank. There are then certain internal infrastructure and capacities necessary before adopting a KYC utility. Examples of essential capacity needed may include[50]:

- *Identification systems (whether developed by national authorities or the private sector).*
- *For primary information that exists in non-English languages, translation services acceptable to correspondent banks.*
- *Other validation/certification that gives comfort to the correspondent banks of the authenticity of the information submitted.*
- *Systems and processes for ongoing updates and maintenance of data in the utilities in a timely manner.*[51]

Although such utilities may have the potential to lower costs, they will not replace all procedures at a bank, and banks are still responsible (in the eyes of US regulators) for any breach in compliance or liability arising from reliance on any third-party tools or methods. Additionally, KYC utilities should not displace institution-specific KYC processes and procedures.

There are certain limitations that global correspondent banks need to keep in mind when considering the use of KYC utilities. Some of these limitations include:

- *Routine or automated updates by the respondent bank are still needed to ensure information is current and accurate.*
- *KYC utilities may not collect all necessary CDD information, so other information may need to be collected bilaterally.*
- *Privacy laws in some jurisdictions may prohibit sharing, storing, or mining of basic information.*

Despite these limitations, KYC utilities can be a highly valuable tool for emerging market banks to take advantage of when approaching KYC/CDD sharing with correspondent banks.

[50] IFC. 2018. A Guide to Respondent Banks: Essential KYC Considerations to Manage Correspondent Banking Relationships in Trade.
[51] IFC. 2018. A Guide to Respondent Banks: Essential KYC Considerations to Manage Correspondent Banking Relationships in Trade.

KYC Utility Vendors

IFC does not endorse a specific KYC utility, and the sample listing of vendors is provided for information purposes only:

- SWIFT has developed the KYC Registry, to which respondent banks can contribute their data at no cost, whereas correspondent banks pay a fee to access the data.
- Thomson Reuters has also developed its own "KYC as a Service" utility solution employed by over 55 global financial institution clients.
- IHS Markit has created a KYC Services platform that has over 140,000 entities represented, including over 80,000 with legal entity identifiers.
- Bankers Almanac has developed a suite of solutions for risk and compliance, including counterparty KYC, due diligence repository, KYC due diligence data file, regulatory views, and ultimate beneficial ownership data.

Local KYC solutions:

- Thomson Reuters has launched a national KYC service in South Africa, where participating financial institutions have access at no charge via a web-based portal.
- African Export Import Bank (Afreximbank) has created African Customer Due Diligence Repository Platform that stores information on African financial institutions and corporations to reduce KYC costs for African clients.

Source: IFC. 2018. A Guide to Respondent Banks: Essential KYC Considerations to Manage Correspondent Banking Relationships in Trade.

LEGAL ENTITY IDENTIFIERS

The international community has recently called for the widespread use of Legal Entity Identifiers (LEIs) which are internationally recognized 20-character alpha-numeric codes that identify distinct legal entities engaged in financial transactions. The LEI is a global standard, designed to be a form of non-proprietary data that is freely accessible to all parties.

The first LEIs were issued in December 2012. Currently, the U.S. and European countries require corporations to use the legal entity identifier when reporting the details of transactions with over-the-counter derivatives to financial authorities. As of December 2018, over 1,300,000 legal entities from more than 200 countries have been issued with LEIs.

Several international bodies, such as Committee on Payment and Market Infrastructures (CPMI) and Wolfsberg Group, point out that wide adoption of LEIs has the potential to significantly reduce false-positive alerts generated by transaction monitoring systems for sanctions and AML/CFT purposes.[52,53] Although the LEI may provide certain benefits related to AML/CFT compliance, it was not designed for AML/CFT purposes, and its potential and limitations need to be investigated further. Additionally, because the LEI does not apply to natural persons, a similar solution for individuals would be required.

The importance of an unambiguous legal entity identifier (LEI) also became apparent after the global financial crisis. Authorities worldwide were unable to identity parties conducting transactions across different markets, regions, and products, which in turn made it difficult for banks to identify trends, evaluate emerging risks, and take corrective action. To combat these difficulties, regulators in collaboration with the private sector have developed a framework that allows for unambiguous identification of entities[54] through the issuance of a unique a 20-digit alphanumeric reference code. Although they were not designed to be used for AML/CFT purposes, they can improve the effectiveness of certain AML/CFT processes, specifically in correspondent banking relationships. The KYC utilities and information sharing described previously require identification of banks or customers included in respective databases. Rather than developing a new standard, the LEI is commonly being adapted as a standard for such utilities.

LEIs are issued in various jurisdictions through local operating units (LOUs), which issue LEIs for a fee and validate the reference data upon issuance and after periodic

[52] CPMI. 2016. Correspondent Banking.
[53] The Wolfsberg Group. 2017. Payment Transparency Standards.
[54] LEIs are for identification of legal entities (including legal arrangements such as trusts) and are not applicable to natural persons, except for individuals acting in a business capacity.

certifications.[55] The Global LEI Foundation (GLEIF) coordinates the LEI system on a global basis, and the list of accredited LOUs can be found on the GLEIF website.[56] The cost of obtaining an LEI as well as jurisdictions served will vary by LOU. Therefore, banks interested in obtaining LEIs for themselves and assisting all the legal entities they do business with should visit the websites of these LEI issuers to determine which ones meet their needs.

ADVANCED TECHNOLOGY APPLICATIONS

When implemented appropriately, adequately, and sufficiently, financial and regulatory technologies (fintech and regtech) may offer banks time- and money-saving solutions to KYC/CDD. Some such technology methods include:[57]

- *Cryptology: Data communication and storage in secure and usually coded form can be used by banks when looking to share KYC/CDD information. Additionally, cryptographic proofs of data stored externally (that is, Dropbox) can be kept.*
- *Big data: Customer data collected from a variety of sources now, including social media data, enterprise customer data, publicly available data, location data, mobile data, web data, and behavior data. When aggregated, such data can give banks a better idea of who the customer is, especially when deciding a customer's creditworthiness.*
- *Artifical Intelligence: Artificial intelligence is the branch of computer science that aims to create intelligent machines. It has become an essential part of the fintech industry focused on programming computers for certain traits such as reasoning, problem solving, and perception. However, computers can often act and react with "intelligence" if they have large data sets (Big Data) relating to the problems assigned. For example, artificial intelligence has the potential to help banks become more efficient in the processing of information by scanning and analyzing legal documents to extract important data points and clauses related to risk.*
- *Machine learning: Machine learning is a subcategory*

e-KYC: The Case of India

India has come a long way in lowering the costs for KYC using electronic means. It uses the Aadhaar system for identifying customers as the basis for its KYC efforts. Aadhar is a unique 12-digit identification number issued by the Indian government to every citizen. The idea behind Aadhar is to have a single, unique identification number on a document, the Aadhar card captures all details, including demographic and biometric information, of every individual resident in India. The Aadhar card does not mandate replacement of existing identification documents, but it can be used to serve as the basis for compliance with KYC norms by financial institutions and other businesses that maintain customer profiles.

A resident Indian can apply for the Aadhar number and card by submitting the existing proof of identity (passport, driver's license, and so forth) and proof of address (phone, power bill, bank statements, and so forth) and by undergoing biometric profiling (fingerprints and iris scan) at any Aadhar center.

Aadhaar became the foundation of some transformative projects within India. For example, in 2014, India launched the Prime Minister's People's Wealth Scheme, which gives low-cost, no-frills bank accounts to the underserved if they can provide details about their identity. From 2014 to 2017, the number of simple bank accounts such as these grew tenfold, from 30 million to 300 million, thanks partly to the availability of Aadhaar authentication.

For correspondent banks, the knowledge that its respondents use a biometric identification system and have access to reliable and up-to-date information on their customers gives them a degree of comfort regarding KYC by their respondents and thus, all other things being equal, makes this relationship more attractive.

Source: Excerpt from The World Bank Group's "The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions," 2018 and https://www.foreignaffairs.com/articles/asia/2018-08-13/data-people

[55] CPMI. 2016. Correspondent Banking.
[56] https://www.gleif.org/en/about-lei/how-to-get-an-lei-find-lei-issuing-organizations.
[57] European Banking Authority. 2018. EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech.

of artificial intelligence. If specific risks are managed properly, this technology can be used to further refine processes for detecting patterns of suspicious transactions by "learning" from experience of detecting true positives.

- *Biometrics: Biometric authentication technologies measure a person's unique and stable biometric features and match them with authorized biometric samples of that same person. This allows for accurate verification of that person's identity with external features unique to them, such as fingerprint, face, iris patterns, or voice. Although the opportunities from biometric authentication are great for both banks and customers, there are legal, security, and reputational risks involved in such technology. It is imperative that banks address all possible risks and be familiar with local laws to ensure that such technology is appropriate not only for the risk assessment within the AML/CFT program but also for the laws and regulations within the institutions' jurisdiction.*

The case study provided here discusses how KYC-related innovations are being used in India and the benefits they offer to respondent and correspondent banks.

Although digital options can and should be used as appropriate, they cannot completely replace AML/CFT processes. The risk and responsibility of adequate policies and procedures, especially in terms of KYC/CDD, falls on the bank itself. All financial technologies should be used in combination with a risk-based approach and in adherence with local laws or data privacy regulations that may restrict certain activities, such as information sharingz.

3.6 Transaction Monitoring

Transaction monitoring involves manual or electronic scanning of transactions based on certain parameters (for example, customer and beneficiary names, and volume, value, country of origin or destination of transactions) to determine if they are consistent with the bank's knowledge of the customer. Transaction monitoring is intended to alert the bank to unusual business relationships and activity, enabling the bank to meet its statutory obligations with respect to reporting potentially suspicious transactions. Banks should have an adequate monitoring system in place, which means the system must be commensurate with the bank's risk profile, size, complexity, and activities.[58] Although it may be appropriate for some small banks to employ manual scanning of transactions, most banks, particularly those that conduct international transactions, are expected to have an automated solution in place which enable them to identify unusual transactions and patterns in a more efficient and effective manner.

The degree and nature of transaction monitoring should be risk based. With this approach, although higher-risk situations may require enhanced monitoring, banks may apply reduced monitoring to lower-risk situations (for example, customers with lower inherent risk, products and services that have strict limits, and lower-risk jurisdictions of customers and transactions).[59,60]

When designing thresholds and risk parameters, the bank should consider customer risk profiles, information collected during its CDD process, and if applicable, any information provided by law enforcement or other authorities to account for any ML/FT schemes identified by them.[61] Monitoring controls can include alert scenarios or setting limits for a particular activity. The system thresholds and parameters are to be assessed by the AML/CFT compliance function and independent audit on a regular basis.

The bank's monitoring system should have a capability to detect transactions with known or suspected terrorists or sanctioned persons or entities. It is strongly recommended that messages associated with wire transfers be subject to ongoing monitoring. In the context of wire transfers, messages MT 103 and MT 202 COV are particularly important as they identify the originator and beneficiary of the wire transfer.

At a minimum, a transaction-monitoring system should have the capability to generate key information for the board of directors and senior management, such as changes in customer profiles. The system should also have capabilities to provide a centralized view of information by customer or product or across group entities.[62] The ability to provide a centralized or enterprise wide view is particularly important when the bank has customers served by multiple business units. This functionality enables the bank to account for all the risks posed by such customers.

---

58 BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
59 FATF. 2017. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. With a Supplement on Customer Due Diligence.
60 FATF. 2014. Guidance For a Risk-Based Approach. The Banking Sector.
61 BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
62 BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

SUSPICIOUS-TRANSACTION REPORTING

Banks are to have procedures and processes for identifying, investigating, and reporting suspicious transactions. These processes should include the necessary automated, semiautomated or manual monitoring systems to flag unusual or potentially suspicious-transaction activity that requires further investigation to determine whether the transactions are suspicious and are required to be reported to the relevant authorities.

Banks must have access to sufficient expertise and resources in order to design and implement the necessary monitoring systems. A critical part of design and implementation of monitoring systems is ensuring they are aligned with the bank's risk assessment results, as well as the criminal typologies related to the products, services, customers, and geographies addressed within the risk assessment and CRR results. Mature processes also include computer-based case management systems that track and document transaction monitoring system output, investigation activities, and suspicious-transaction report (STR) filing or nonfiling.

Personnel responsible for identifying, investigating, and reporting suspicious transactions should be well trained on internal policies, procedures, and legal requirements (for example, how to prepare STRs) and provided with necessary resources and guidance on how to recognize suspicious activity based on applicable criminal typologies and schemes.[63]

Financial institutions and their employees should be protected by law for breach of any restriction on disclosure of information related to filing an STR if the institutions report their suspicions in good faith and should be prohibited by law from disclosing that an STR is being filed with the FIU.

It is imperative that financial institutions and their employees not disclose or "tip off" the fact that a suspicious-transaction report or related information is being filed. Tipping-off a customer is a criminal offense in many countries.

Financial Institutions And Their Employees Should Be Protected By Law From Criminal And Civil Liability For Breach Of Any Restriction On Disclosure Of Information Related To The Filing Of A Suspicious-Transaction Report.

When designing the process for identifying, investigating, and reporting suspicious activity, banks should consider coordinated information sharing. Branches and subsidiaries should be able to provide the head office with information relating to high-risk customers and any STRs filed on them as part of the enterprise risk management framework. Due to the confidential nature of STRs, however, a bank should take steps to protect such information since there may be local laws in which a bank can be liable for direct or indirect disclosure, whether by its controlling company or head office if an STR itself, or even just the fact that an STR was filed becomes public. Typically the recipient head office, controlling entities, or related parties may not disclose any STR information or the fact that such a report has been filed. Some jurisdictions do allow institutions to disclose—without government approval the underlying information relating to the STR (that is, information about the transaction[s] or type of activity reported) as long as the information does not explicitly reveal that an STR was filed and that is not otherwise subject to disclosure restrictions. For these reasons, the bank, as part of its anti-money laundering program, should have written confidentiality agreements or arrangements in place specifying if STR filings are shared that the head office or controlling company must protect the confidentiality of the STR through appropriate internal controls.

As discussed in Section 3.5 Customer Due Diligence, when certain triggering events occur, such as the bank filing an STR on its customer, the bank should reassess the potential risk posed by this customer and reevaluate the risk rating. Also, when multiple STRs are filed on a customer or an STR alleges serious criminal activity, the institution must immediately take appropriate steps to mitigate the risk, for example by (i) requiring an approval from an AML/CFT officer or another high-level decision maker within AML/CFT compliance function to continue the business relationship, (ii) subjecting the customer to enhanced monitoring and setting up lower thresholds, or (iii)

[63] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

Practical Tips for Fine-tuning AML/CFT Transaction Monitoring Systems[62]	
Selection of scenarios/rules	• Perform ML/FT risk assessment for the identification of red flags or the type of unusual/suspicious behavior to be monitored for, given the inherent risks associated with the bank's customers, products, services and geographies in scope • Understand scenarios/rules logic (risk mitigation, scenario focal entity, frequency, lookback period, and tunable parameters) and map red flags to the scenarios/rules offered by the transaction monitoring solution • To the extent some risks cannot be addressed by the automated transaction monitoring tool, identify an alternative approach to implement mitigating controls (for example, manual monitoring)
Identify customer segmentation to apply to scenario/ rules	• Consider segmenting customers such that more focused and enhanced scenario/rules logic can be applied • Use KYC information to segment customers into population and peer groups for the purposes of targeted monitoring (for example, net worth of the customer, business/personal, types of business) • Assess how CRRs and geography risk ratings used by the institution can be adopted and used by the monitoring platform rules for further segmentation • Determine how customer population/peer groups will "inform" the transaction monitoring scenarios/rules
Initial threshold setting/ preproduction tuning	• Establish clear protocols and procedures for preproduction tuning, including sampling approaches, sample scoring, and risk tolerances (risk tolerance defines the level of risk exposure that is acceptable to the bank in relation to achieving a specific scenario's/rule's objective) in advance of the initial tuning • In a test environment, perform statistical analyses to identify distributions and statistical properties for each scenario/rule using de minimis (low value) thresholds using any defined population/peer groups • Identify initial thresholds for each scenario/rule based on the distribution of alerting activity (for example, 95th percentile) • Threshold fine-tuning: perform statistical sampling of test alerts above the line and below the line of the initial threshold and provide a sample test alert around the threshold to the financial investigations unit for high-level investigation (the financial investigations unit should be trained on rules and risk coverage before sampling) and scoring ("false positive," "of interest," "high-interest") • Based on the results of the sample scoring and the bank's risk tolerance, select additional samples slightly higher/lower than the initial threshold and repeat sampling and investigation of alert around the new threshold, as required • Set final threshold at a level that provides coverage of risk within the bank's risk tolerance (that is, at a level where the number of true-positive or of-interest alerts missed is low) • Revisit all initial parameters set within 6 to 12 months, using production history for tuning
Tuning of production thresholds	• Establish clear protocols and procedures for production tuning • Perform production tuning in a similar manner to preproduction tuning • Perform a distribution analysis of historical alerts, cases, and STR filings for each rule • Depending on the distribution of activity, perform above-the-line and below-the-line sampling and scoring to reduce the occurrence of false-positive alerts or minimize not capturing true-positive alerts; repeat sampling, as necessary, at different threshold values • Based on sampling results, adjust threshold values, as needed
Documentation	• Document the process, methodology, and evidence and outcome of tuning processes used

restricting the customer's transactions to a limited number of products/services. If the risk cannot be mitigated, the bank should consider closing the account.

[64] Excerpt from FST. 2010. AML Rules Optimization to Enhance Transaction Monitoring.

RELIANCE ON THIRD PARTIES

If a bank uses an externally sourced transaction monitoring system, it must take necessary measures to ensure that the system has adequate parameters and addresses the needs of the bank. Even if the system was purchased externally, the system thresholds and parameters should be assessed by the AML/CFT compliance and independent audit functions on a regular basis.

If the bank uses third parties/agents to perform some of the CDD, the transaction monitoring system should also cover what is performed by such third parties/agents.[65]

EMERGING TECHNOLOGY SUPPORTING TRANSACTION MONITORING

The emergence of new fintech and regtech provides great potential for improving the ability of banks to detect and report suspicious transactions. In its report on Deploying Regtech Against Financial Crime, the Institute of International Finance (IIF) Working Group stated that new technologies can allow for:

- *"More effective detection of suspicious transactions and activities through increasingly accurate detection systems and technologies for faster, more secure and more efficient data sharing;*
- *Reduced human error due to automation of part of the process;*
- *Increased security of interactions between banks and their clients, thus reducing vulnerability to fraud; and*
- *More efficiency at banks across the financial sector as costs of compliance are brought down."*[66]

Currently, several technologies available in emerging markets can improve banks' processes related to identifying, investigating, and reporting suspicious activity:[67,68]

- *Big data technologies, including storage repository (for example, clouds, data lakes) and data processing engines, can provide banks with a central infrastructure that can store large amounts of information. Big data infrastructures can hold vast amounts of data relevant to AML/CFT investigations, such as transactions metadata; information from external, sources including unindexed websites routed through many layers of anonymity to conceal an operators' identity and that are not accessible to everyday Internet users (known as "the deep web") ; public sources; and KYC utilities.*
- *Machine learning technologies can be extremely useful in detecting unusual activity. Such advanced software can apply detection rules to vast volumes of data, identify complex patterns and nonlinear relationships, and analyze unstructured data sources. When it is applied to transaction monitoring, it can detect suspicious activity more accurately. For example, if a software is programed to "red flag" suspicious activity, the outcome of FIU investigations can be fed back into a program such that confidence levels can be improved by the software itself and false positives can be reduced. These technologies can generate suspicious activity reports by automatically detecting patterns of unusual activity that would be difficult to produce via human monitoring.*
- *Robotics, the use of artificial intelligence to automate manual tasks, can be used for certain processes related to AML/KYC investigations. Although investigation analysts still have an important role in the investigative process, robotics has the potential to free up compliance personnel's time, allowing them to focus on analytical work and complex investigations. Automation can also limit human error and human bias in decision making.*

The effectiveness of available technologies will depend on the capacity of banks and require a coordinated action between banks, central banks, and other regulators.[69] The case study that follows outlines the efforts undertaken by Mexican authorities related to transaction monitoring and customer due diligence.

---

[65] FATF. 2017. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. With a Supplement on Customer Due Diligence.
[66] IIF. 2017. Deploying Regtech Against Financial Crime.
[67] IIF. 2017. Deploying Regtech Against Financial Crime.
[68] The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.
[69] The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

Cross-Border Transactions and a KYC Utility: The Case of Mexico

Mexican authorities are developing two databases that will be combined: a database for cross-border transactions and a KYC utility. The database for cross-border transactions records all domestic wire transfers in foreign currency, as well as cross-border wire transfers originating in Mexico, irrespective of their size. Every financial transaction that crosses the border must be reported. For each transaction, banks report basic information about the ordering customer, the recipient bank, the beneficiary of the transfer, the amount sent, the currency sent, and more. It is noteworthy that the database does not capture inbound operations that originate abroad at this point. Inbound transactions will be captured in late 2018.

The goal of the database for cross-border transactions is to enable banks to assess the risk of their customers in a more holistic way. Banks have only a partial view on the financial profile of their customers. They have information on the transactions that they conduct on behalf of their clients but not on those transactions conducted by other entities. Through the database, each bank can see the forest—not only the trees.

The output can be queried at any time by the banks and will comprise information on a customer's transactions from the previous year, which will be updated daily. Although no other information needs to be gathered by the banks, the database will foster the quality of ML/FT risk management by providing additional information on transactions that is not accessible otherwise. In addition, the database provides detailed information on cross-border transactions and domestic wire transfers in foreign currency. The system also defines for each client a specific code (ranging from 1 to 5) corresponding to the client's level of activity, which should lead the bank to conduct extra due diligence and seek more information on the client.

Accuracy and consistency of data are of paramount importance. For the database to accurately summarize the transactional activity of a sender in the financial system and gain trust among banks as a reliable source of information, reported data must be high quality. Therefore, Banco de Mexico (BdM) established a comprehensive framework to encourage banks to report consistent and authentic data combined with measures to rectify already reported data and avoid recurrences.

The database, although not yet operational, has a wide scope, is resource intensive, and relies on a proper information technology infrastructure. Whereas the usefulness of a database with these dimensions is clear, this database may not be an option for low-capacity countries. There are some preconditions to be met, including a reliable and widely distributed information technology infrastructure, sufficient capacity to maintain the system (BdM developed an in-house algorithm to monitor inconsistencies and errors), and strong security systems to protect against cyber threats.

Source: Excerpt from the World Bank Group's "The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions," 2018.

3.7 Reporting

An essential part of all banking jurisdictions' anti-money laundering regimen is providing authorities reports on important financial transactions. These bank regulatory requirements typically include suspicious-transactions reports and large currency transaction reports. To meet these obligations, banks must have adequate policies, procedures, and systems in place to be able to provide the required reports to appropriate governmental agencies (external reporting). The financial intelligence value of these reports is best leveraged internally through MIS reports that enable the bank to manage ML/FT risks (internal reporting).

EXTERNAL REPORTING

External reporting typically involves reporting of (i) suspicious transactions and (ii) cash (currency) transactions exceeding a certain threshold to relevant authorities (for example, FIUs).

SUSPICIOUS-TRANSACTION REPORTING

As discussed within the transaction monitoring section, banks should have procedures and processes for reporting suspicious transactions. STRs provide valuable intelligence to law enforcement authorities. Banks should have sufficient expertise, resources, and the necessary monitoring to be able to understand and comply with the reporting requirements, including timely filing of the reports.

CASH (CURRENCY) TRANSACTION REPORTING

Currency transaction reporting and government analysis of these activities, while not a FATF standard, have become an increasingly important source of financial crime intelligence. In response to these filing requirements and given the high value to authorities, banks should have procedures and processes for identifying, aggregating, and reporting cash (currency) transactions to appropriate governmental agencies, as mandated by national laws. Banks should have computer-based systems supporting this reporting process. The design of such systems must incorporate appropriate regulatory requirements that enable the bank to meet its reporting obligations, including timely filing of the reports.

Personnel responsible for identifying and completing cash (currency) transaction reports should be well trained on internal policies and procedures. Additionally, banks with operations in multiple jurisdictions should be aware that cash (currency) reporting requirements vary from country to country and must ensure that the compliance personnel responsible for such reporting are fully conversant with the local regulatory requirements.

INTERNAL REPORTING

Internal reporting of AML operational performance and output is critical to the overall bank risk management and AML/CFT risk management processes. AML/CFT-specific MIS reports typically cover key information such as:

- *significant AML/CFT regulatory changes,*
- *regulatory examination and internal audit results,*
- *risk assessment/bank risk profile changes,*
- *statistical data on high-risk accounts,*
- *STR filing trends,*
- *potential backlogs in timely STR or cash (currency) transaction report filings,*
- *staffing levels, and*
- *potential impact of new products and service offerings in the pipeline.*

All MIS reports should be made available and commonly discussed during bank risk committee or compliance operations meetings and include all relevant stakeholders, including senior executive management, first-line executives, CRO, CCO, and AML/CFT officer. The reports must be sufficiently detailed and cover main Key Risk Indicators (KRIs) to facilitate the management's assessment of the state of AML/CFT risk exposures. More importantly the reports must cover the effective operation of the AML/CFT control environment, as well as the early identification of any issues within AML/CFT operations or the business unit's execution of AML/CFT requirements. The table the follows provides examples of information to be included in MIS reports.

MIS Report (For Illustrative Purposes Only)	
Key Topic	**Examples of Information to be Included in the Report**
Regulatory environment **Results of internal testing Regulatory examination results**	• AML/CFT regulatory changes • Internal audit testing results • Regulatory examination results • Remediation action plan and progress reports
Risk assessment	• Potential changes in bank's risk profile, including additional products and services, new higher-risk customers, and potential higher-risk geographies
High-risk customers (HRCs)	• New HRCs onboarded for the month • Total number of HRCs • Percentage of HRCs against customer base • Breakdown of HRCs by customer type (for example, PEPs, casinos) • Comparison of number of HRCs with that of previous month
Suspicious-transaction reports (STRs)	• STRs filing trends, number and percentage change of STRs filed the last 3 months and prior year • Number of STRs filed late • Number of investigations in process versus number of investigations completed on a weekly basis for past 2 months • Number of investigations not yet completed in prior week for the past 2 months
Transaction monitoring alerts	• Number of alerts and investigations in the current queue this month (for example, number of open and closed alerts and investigations) • Number of alerts and investigations generated and closed last month • Number of alerts and investigations generated and closed in the prior 2 months • Identify the differences each month from generated and closed to quantify the number of overdue alerts and investigations (for example, backlogs)
Customers with outstanding EDD/ CDD/identification verifications	• Number of new customers and number of identification verifications completed • Scheduled number of EDD requiring updating and number of EDD refreshes completed • Scheduled number of CDD requiring updating and number of CDD refreshes completed • Total number of outstanding EDDs/CDDs requiring completion • Percentage of HRC with incomplete EDD
Other compliance matters	• Training schedule and completion ratio • Staffing levels versus staffing plan • Key leadership/staffing shortages in critical compliance and operations departments

3.8 Communication and Training

Effective AML/CFT risk management is not possible without clear and routine cross-organizational communication and the training of appropriate personnel. Where allowable, banks are expected to develop mechanisms for sharing relevant information across the entire institution. This starts with a strong risk management culture and the tone established by the board of directors and flows through senior management into middle management as well as line management and staff. Mature communication and risk management infrastructures include compliance and AML/CFT executives in bank strategic discussions and operational committee meetings. This allows critical and timely AML/CFT operational, compliance, and regulatory changes and issues to be discussed and addressed at a strategic level and ensures buy-in at all levels of the institution. This structure also allows

all departments with pertinent information that may be useful to the AML/CFT compliance staff to freely flow that information to the necessary executives. This timely sharing of information creates a stronger and more integrated control and risk management environment. The stronger and more transparent the control and risk management environment, the more likely the AML/CFT program effectiveness will be viewed favorably by a correspondent bank.

Training of appropriate bank personnel from the board of directors to operational staff is a key component to an effectively operating AML/CFT program. The scope and frequency of training should be tailored to the level and nature of risk present in the bank and the risk factors to which employees are exposed because of their responsibilities. Employees exposed to the greatest risk factors due to their roles and responsibilities should be expected to complete at least 40 hours of continuing professional education training annually with specialized course work in AML/CFT risk management.

These specialized AML/CFT training courses are offered by various professional organizations, such as the Association of Certified Anti-Money Laundering Specialists (ACAMS), Association of Certified Fraud Examiners (ACFE) and American Bankers Association (ABA). Upon successful completion of course work and passing an examination, individuals obtain a professional certification/designation, such as certified anti-money laundering specialist (CAMS), certified fraud examiners (CFE), or certified anti-money laundering and fraud professional (CAFP). Further, adequate training is required to ensure that bank personnel understand the AML/CFT processes they are required to follow, as well as the risks the processes are meant to mitigate, and the consequences of those risks. Banks should ensure that all relevant personnel are adequately trained on AML/CFT policies, procedures, and processes and such procedures are made easily available to them.

Training for new employees should occur as soon as possible after being hired, and refresher training is to be provided to ensure that employees' knowledge is kept up to date. It is good practice for banks to retain records of their training sessions, including attendance records and relevant training materials used.

Training received by bank personnel should be:[70]

- ***High quality**, relevant to the bank's policies, procedures, controls, current regulatory requirements, ML/TF risks, and the bank's business activities;*
- ***Obligatory** for all relevant personnel (including board of directors, senior executives, middle management, and operational staff);*
- ***Effective**, including a mix of discrete fact-based training that covers policies, procedures, and regulation requirements (for example, commonly executed through computer-based programs), and more interactive (in-person) training sessions (for example, in-house training sessions or conferences or seminars) that discusses the more challenging qualitative aspect of risk-based AML/CFT compliance. As part of the effectiveness expectation, requiring staff to pass a test on the subject matter provided holds employees accountable for obtaining and retaining this knowledge. Monitoring levels of compliance with the bank's AML/CFT controls and identifying where staff are unable to demonstrate the level of knowledge expected are valuable to the process of identifying additional training needs;*
- ***Tailored** to a particular job function and lines of business within the bank;*
- ***Ongoing**, meaning that AML/CTF training should be regular, relevant, and not a one-off exercise when staff are hired; and complemented by periodic AML/CFT information and timely updates that are disseminated to relevant staff as appropriate.*

[70] FATF. 2014. Guidance For a Risk-Based Approach. The Banking Sector.

Guidance for AML/CFT Training

When developing AML/CFT training for employees, a financial institution should consider the following factors:

- Does the financial institution provide mandatory AML/CFT training that includes:
  - Identification and reporting of transactions that must be reported to government authorities;
  - Examples of different forms of money laundering and terrorist financing involving the financial institution's products and services;
  - Internal policies for controlling money laundering and terrorist financing;
  - New issues that occur in the market (for example, significant regulatory actions or new regulations); and
  - Conduct and culture?
- Is this mandatory training provided to all relevant personnel, including the board, senior management, all three lines of defense, and third parties to which AML/CFT activities have been outsourced and contractors/consultants)?
- Is the training targeted to specific roles, responsibilities, and high-risk products, services, and activities?

Source: Excerpt from The Wolfsberg Group. 2018. Correspondent Banking Due Diligence Questionnaire.

3.9 Continuous Improvement and Testing

The AML/CFT compliance function should have responsibility for ongoing monitoring of the fulfilment of all AML/CFT duties by bank employees. This implies assessment of AML/CFT compliance, review of exception reports, and reporting of main compliance failures to the board and/or senior management.

Compliance assessment should be constructed to validate that key assumptions, data sources, and procedures used in measuring and monitoring AML/CFT compliance risks can be relied upon on an ongoing basis. AML/CFT compliance assessment should be program wide and risk based and should include main AML/CFT compliance aspects, such as:

- *CDD processes;*
- *STR reporting;*
- *Cash (currency) transaction reporting;*
- *Training;*
- *Systems supporting AML/CFT compliance (for example, transaction monitoring, customer information management) and*
- *AML/CFT methodologies used by the bank (for example, risk assessment, CRR, product risk rating, and country risk rating).*

As part of the bank's continuous improvement program, robust AML/CFT compliance assessments play a key role in self-identifying weaknesses in existing AML/CFT controls and remediating identified deficiencies and thus are essential to sustaining effective AML/CFT risk management.

3.10 Internal and External Audit

Internal audit, as described, is the third line of defense that independently evaluates the AML/CFT program and processes carried out by the first and second lines of defense. The expertise and independence of the party testing the AML/CFT program (whether internal or external) is paramount. Senior management is to ensure that auditors are qualified, independent, and do not have conflicting business interests/responsibilities that may influence the outcome of the audit. To further promote the independence of the audit-testing function, the board and senior management should ensure that all AML/CFT audit reports (whether internal or external) are directly provided to the board and audit committee.

At a minimum, independent audit testing should include an assessment of the following components of the AML/CFT program:

- *Governance and oversight and organizational structure;*
- *Risk assessment;*
- *Written policies and procedures;*
- *Customer identification, customer due diligence, and enhanced due diligence;*
- *Transaction monitoring;*
- *Suspicious-transaction and currency-transaction reporting;*
- *Management information systems reporting;*
- *Training;*
- *AML/CFT technology platforms used to support the AML/CFT program;*
- *Use of third parties for AML/CFT-related processes;*
- *Record retention; and*
- *Applicable legal requirements not previously mentioned.*

Independent audit testing should also include sample testing of key controls and processes, such as customer identification, CDD/EDD, transaction monitoring, suspicious-transaction and currency-transaction reporting, and others, as applicable. Additionally, transaction monitoring tool(s) and other models/methodologies supporting AML/CFT compliance (for example, CRR and product risk rating) should be subjected to an independent validation to ensure they operate as intended.

Personnel within the bank's internal audit function must have the requisite knowledge, be appropriately trained, and not be involved in developing, implementing, or operating any first- or second-line of defense functions. Senior management must ensure that the internal audit function is allocated sufficient resources (adequate number of employees that are knowledgeable and have required expertise, access to necessary systems, information and bank personnel). The volume of resources depending on the size and complexity of the bank.

Frequency, scope, and methodology of AML/CFT audits should be commensurate with the bank's risk profile. Periodically, internal auditors should conduct AML/CFT audits at the enterprise wide level. Mature programs are typically subjected to an annual independent testing or once every 12 to 18 months. In addition, internal auditors should be proactive in following up on any remedial actions arising from independent audit or regulatory findings and periodically report to the board or applicable committee on the status of those corrective activities. The processes carried out by the internal audit function should be formally documented in written procedures.

External auditors can also be used in evaluating banks' AML/CFT programs. If a bank engages external auditors to evaluate the effectiveness of the AML/CFT program, the bank should 1.) ensure that the scope of the audit adequately addresses the bank's ML/FT risks; 2.) the staff expertise needed is assigned to the engagement; and 3.) sufficient resources are provided. A bank must also exercise appropriate oversight of such engagements. Finally, many correspondent banks will be reassured as to the effectiveness of an AML/CFT program if the respondent bank is willing to share their external audit reports on a confidential basis.

Chapter 4
Dealing with your Correspondent Bank and Other Stakeholders

Understanding a Correspondent Bank's Perspective

Understanding a correspondent bank's perspective and aligning your practices with the global standards are essential for ensuring that CBRs are maintained.

In recent years, the international community and local authorities have expressed concerns about correspondent accounts being used to facilitate illicit activities and have urged banks to implement necessary control measures to inhibit or prohibit accounts from being used to launder money and finance terrorism. Recent enforcement actions including significant fines imposed on banks in the United States, Europe, and elsewhere are partially due to the inability of such institutions to conduct adequate due diligence, suspicious-activity monitoring, and reporting on foreign correspondent bank account activity. This has heightened awareness around the need for banks to re-evaluate all their correspondent banking relationships.

Due to these regulatory actions as well as post-2008 profitability/business considerations, a more rigorous risk threshold, customer onboarding, and due diligence process has emerged. Global and regional correspondent banks now assess multiple aspects of ML/FT risks associated with their current relationships and potential new relationships. Many have implemented more robust controls and due diligence processes based on external regulatory expectations and international standards. These due diligence assessments typically include the following risk indicators:[71]

1. *The characteristics of the respondent bank*
   - *The respondent bank's major business activities, including target markets and overall types of customers served.*
   - *The respondent bank's management and ownership, including beneficial owners.*
   - *The respondent bank's governance framework and how AML/CFT is treated in it.*
   - *The respondent bank's AML/CFT policies and procedures, particularly CDD procedures. This may include evidence of rejecting PEPs or other high-risk customers and whether the policies and procedures were gapped against U.S. and EU standards.*
   - *Any civil, administrative, or criminal actions applied to the respondent bank by any court or regulator.*
2. *The environment in which the respondent bank operates*
   - *The jurisdiction in which the respondent bank and its subsidiaries and branches are located.*
   - *The effectiveness of AML/CFT laws and regulations in the respondent's country.*
3. *Whether banking services will be used via nested correspondents or payable-through accounts*
   - *Payable-through accounts[72] are largely prohibited by most/all correspondent banks at this time because of the inherent AML risk. Nested correspondent banking[73] are also perceived to have a higher risk by correspondent banks because they are less transparent and make it hard to determine who the ultimate customer is and what due diligence was conducted on the ultimate customer.*

[71] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[72] Defined as the use of a bank's correspondent relationship by the respondent bank's customers who can directly access the correspondent account to conduct business on their own behalf.
[73] Defined as the use of a bank's correspondent relationship by a number of respondent banks in a cascade.

In addition to performing normal CDD, it is recommended that correspondent banks perform additional due diligence in relation to cross-border correspondent banking. The additional measures include the following:

- *assessing the respondent bank's AML/CFT controls; and*
- *with respect to payable-through accounts, becoming satisfied with the respondent bank's CDD conducted on customers having direct access to the respondent bank and that it can provide relevant CDD information upon request to the correspondent bank.*

In addition, correspondent banks are prohibited from entering or continuing relationships with shell banks and need to satisfy themselves that their respondents do not maintain relationships with shell banks.

In addition to performing due diligence of a respondent bank at onboarding, correspondent banks are expected to conduct ongoing monitoring of respondent banks to detect transactions that are not consistent with the purpose of the services provided or contrary to the agreements between correspondent and respondent banks. The level of ongoing monitoring should again depend on the level of risk posed by the respondent bank. For example, payable-through accounts should be subject to enhanced monitoring.

As part of ongoing suspicious activity monitoring, when there are concerns about certain alerted activity, the correspondent should issue a request for information (RFI) on that transaction to the respondent bank.

It should be noted that, although this is becoming rare, in certain jurisdictions correspondent banks are still expected to conduct due diligence and monitor for suspicious activity not only of respondent banks but also of their customers.

These international standards and due diligence expectations with respect to correspondent banking were embraced by domestic regulators in the United States and the European Union, where a significant number of major correspondent banks are based. The European Union's Fifth Anti-Money Laundering Directive establishes correspondent banking standards that are closely aligned with the FATF guidance. U.S. regulations are also aligned with the international guidance; however, some of the additional requirements imposed on U.S. banks are highlighted below[74]:

- *U.S. banks that maintain foreign correspondent accounts must maintain records in the United States identifying the owners of such foreign banks. U.S. banks must also record the name and street address of a person who resides in the United States and who is authorized and has agreed to be an agent to accept service of legal process. This information must be obtained within 30 calendar days of establishing the account and at least once every 3 years thereafter and reviewed for reasonableness and accuracy.*
- *U.S. banks are required to conduct EDD at onboarding and on an ongoing basis on foreign banks operating under the following:*
  - *An offshore banking license.*
  - *A banking license issued by a foreign country that has been designated as noncooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member.*
  - *A banking license issued by a foreign country that has been designated by the secretary of the treasury as warranting special measures because of money laundering concerns.*

Communicating with Your Correspondent Bank and Other Relevant Stakeholders

As mentioned at the onset of this chapter, understanding correspondent banks' perspective and aligning your bank's practices with the global standards are essential for ensuring that CBRs are maintained. Respondent banks have to consider supplementing their focus on designing, implementing, and demonstrating a strong AML/CFT program with frequent dialogue and relationship building with correspondent bank(s) and other relevant stakeholders, such as regulators, auditors, and professional associations. The following communication and AML/CFT risk management strategies may be helpful.

[74] This discussion is included for informational purposes because U.S. banks have an extensive number of correspondent bank relationships, and thus emerging market banks should be aware of the unique U.S. requirements.

IMPROVING THE INFORMATION FLOW TO CORRESPONDENT BANKS

As mentioned, correspondent banks are required to collect and maintain sufficient information about the respondent bank. Their own ability to manage CBRs depends on quality, timeliness, and cost of obtaining information they receive from their respondents. Maintaining CBRs is challenging and expensive for both sides. Respondent banks should therefore strive to employ systems and tools that can facilitate information exchanges, specifically address the current documentation expectations, and enable cost savings that accrue to both parties.

Automation is a necessary step in this direction. Some small banks still have manual processes for customer onboarding and ongoing monitoring. This can hamper information flow and at times the understanding of customer transaction activity. Yet without sufficient explanations on how paper-based CDD processes can also be effective, the correspondent bank may question the strength of a respondent bank's ML/FT risk management system. This may well lead to a CBR account closure.

Mature AML/CFT programs leverage technology for important financial crimes processes, including CDD/EDD and suspicious-activity monitoring systems. Some of the tools that facilitate information exchange (for example, KYC utilities and LEIs) are discussed in previous chapters. It is worth the investment in time, during the respondent bank's ongoing discussions with correspondent banks, to find out if they use any of these industry-leading KYC utilities. Additionally, respondent banks should consider the use of a KYC utility that incorporates the Wolfsberg Correspondent Banking Due Diligence Questionnaire used by many international correspondent banks to assess the respondent's AML/CFT risk.

Such tools can make it easier to manage CBRs for both sides as most of the information requirements are predefined. This can facilitate information flow and lower the costs of producing such information. Jurisdictions with a smaller number of respondent banks may consider newer initiatives, such as pooling with other banks to develop automated suspicious-activity monitoring solutions or access relevant commercial databases.

Additional communication strategies that respondent banks should consider include setting up working groups that include banking authorities, if possible, and correspondent banks. This may allow for all stakeholders to reach a common understanding of regulatory requirements in foreign jurisdictions, develop or follow AML/CFT best practices, or develop additional communication channels with foreign supervisors and pertinent correspondent banks.[75]

SHARING OF BEST PRACTICES

Sharing of best practices between correspondent and respondent banks and between respondent banks themselves can support the comprehensiveness of the jurisdiction's overall AML/CFT regimen. This sharing can also assist respondents in identifying potential gaps in their AML/CFT risk management practices and expedite corrective actions to support maintenance of CBRs. Respondent banks should consider taking a proactive approach in communicating with their correspondent banks to gain an understanding of correspondents' risk tolerance and best-practices expectations. Respondents should use this information to enhance their AML/CFT controls and align them more closely with international standards (for example, FATF, Basel, Wolfsberg) since these are the standards that many international correspondent banks look to as best practice.

Ensuring your AML/CFT compliance personnel are aware of and trained on international standards and best practices is critical to proactively ensuring you are meeting current correspondent banks' and international AML/CFT expectations and retaining your CBRs. Respondents should be proactive in reaching out to their correspondents if they need assistance in interpreting global standards or require a targeted training.

One bank indicated that its chief compliance officer's extensive experience in a large U.S. bank was instrumental to maintaining a strong relationship with that bank. It allowed the respondent bank to adopt a risk-based framework similar in design to the U.S. bank's risk framework, and the personal relationship helped ensure a degree of trust.

Source: The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

[75] The World Bank Group. 2015. Withdrawal from Correspondent Banking: Where, Why, and What to Do About It.

Example: Standard Chartered Bank Assistance to Respondent Banks

Standard Chartered Bank provides assistance to its respondent banking clients in a number of ways. As part of "engagement visits," financial crime compliance experts visit the clients to share the latest international regulatory developments in relation to money laundering and other financial crimes and share ideas on what a good compliance program looks like.

A variation of the engagement visit is the "deep dive," in which the Standard Chartered Bank assesses how the client respondent bank is doing on a number of different facets of financial crime compliance, such as policies, screening procedures, organizational structure, governance, and training. The bank advises its clients where they are deficient, and the two parties agree on ways to improve.

Standard Chartered also organizes in-country "correspondent banking academies," which are typically, 1-or 2-day events held for clients and regulators in country. During the academies, case studies are shared and best-practice standards exchanged on customer due diligence and ways of identifying and preventing financial crime. Finally, the bank also holds "regional correspondent banking academies," which are similar but broader in scope and aimed at a more senior level of compliance staff.

Source: http://growthcrossings.economist.com/article/scperspectives-promoting-financial-inclusion-in-correspondent-banking/.

COMMUNICATING WITH DOMESTIC REGULATORS AND INTERNATIONAL ORGANIZATIONS

In assessing the risk of a respondent bank, correspondents routinely consider the risk profile of the country in which the respondent bank is based. The FATF standards require countries to assess their ML/FT risks (for example, national risk assessment) and develop actions to mitigate identified risks. Respondent banks should engage in dialogue with domestic authorities about the importance of conducting and publishing national assessments to demonstrate the country's commitment to AML/CFT risk management and the positive impact the national assessment may have on CBRs. Additionally, respondent banks should consider reaching out to international organizations such as the World Bank that have a record of providing technical assistance to emerging-market banks and domestic authorities. For instance, the World Bank Group has developed a tool to assist countries in performing such a national ML/FT risk assessment. This WBG tool has already been used in more than 80 jurisdictions.[76]

Banking organizations are encouraged to foster closer relationships and to open lines of communication with FIUs and regulators. FIUs have a pivotal role and are an essential component in the international fight against money laundering, financing of terrorism, and other financial crimes. FIUs are national agencies established by governments that receive reports of suspicious transactions from banks and other persons and entities, analyze them, and disseminate the resulting intelligence to law enforcement agencies. Similarly, bank regulatory agencies play an important role in ensuring the safety and soundness of the financial system and that the institutions supervise are not used as conduits for money laundering and terrorist financing. As the use of correspondent banking services continues to receive heightened focus, it is important that banks develop good relationships with the FIUs and regulators. With regulations implemented after the financial crisis of 2007-2008, the goal was to provide more safety and stability to the financial system. Regulators around the world are working toward increased information sharing as well as a global harmonization of compliance standards. As such, the basic features of the FIU should be consistent with the supervisory/regulatory framework of a country.

[76] The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

Improvements to AML/CFT Regimens: The Case of Somalia

To mitigate the risks associated with the loss of CBRs, authorities can consider a range of actions that seek to foster higher standards of transparency and compliance with international financial standards from banks and MTOs. Drafting AML/CFT regulations tailored to a specific sector such as MTOs can greatly improve the formalization, transparency, and compliance of actors who operate in sectors vital to the economy, such as remittances. In that regard, consider the case of Somalia.

The population of Somalia is heavily dependent upon remittances from abroad. Each year, the Somali diaspora remits approximately $1.3–$1.5 billion to relatives and friends in Somalia. In May 2013, a U.K. bank said it intended to close the bank accounts of the Somali remittance company Dahabshiil and approximately 100 other money transfer companies in Somalia. This action followed a corporate decision to de-risk from certain business lines with perceived higher risks of ML/FT. Because remittances are estimated to account for 24 to 45 percent of Somalia's GDP, the threatened withdrawal of the U.K. bank and other banks providing correspondent banking to Somalia raised significant concerns.

In response, the federal government of Somalia with the technical assistance of the World Bank and other international partners is undertaking a policy and institutional reforms program. The "Supporting Remittances Flows to Somalia Project," backed by funding from the United Kingdom, includes measures to improve the formalization, transparency, and compliance of the remittance providers in Somalia. The project supports the efforts of the Central Bank of Somalia (CBS) to begin formal supervision of the Somali MTOs with the assistance of a "trusted agent" (an external firm procured by the World Bank) to work alongside the CBS for 4 years to establish on-site and off-site supervision of MTOs. In March 2016, the World Bank selected the Norwegian firm Abyrint as the trusted agent.

To strengthen the regulatory framework for the MTO sector, the World Bank worked with the Central Bank of Somalia to draft MTO regulations. The regulations focus on two key areas: (i) regulations for operation purposes, including provisions for, among others, customer due diligence, record keeping, ongoing monitoring, reporting, internal controls, consumer protection and risk management, which would apply to all registered and licensed MTOs operating in Somalia; and (ii) regulations for customer registration, which would apply to customers (individuals and businesses) of all MTOs to ensure everyone a fair and equal chance at succeeding. The trusted agent will work with the CBS to ensure that the MTOs and their agents comply with the regulations and meet the requirements on an ongoing basis.

Source: The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

EXTERNAL INDEPENDENT ASSESSMENT OF AML/CFT PROGRAMS

An approach that correspondent banks are increasingly requesting is for an independent assessment of the respondent bank's AML/CFT program. In this way, a respondent bank can provide an independent assessment of the quality and effectiveness of its AML/CFT program. This can also provide the correspondent bank(s) more comfort with the risk exposures at the respondent bank and risk-mitigation controls. When undertaking this option, the respondent banks must engage a reputable firm with the expertise and experience to credibly assess the effectiveness of the respondent's AML/CFT controls. Communicating the results of such testing or assessment and any corrective action to current or prospective correspondent banks, should increase their level of trust and comfort with onboarding or maintaining the CBR.

HANDLING TERMINATION NOTICES

Ongoing productive dialogues; profitable and well-managed relationships; and implementation of mature AML/CFT risk management programs are expected to reduce the likelihood a bank will receive a correspondent bank termination notice. At a minimum, a bank acting in this way should be given an opportunity to address any serious concerns a correspondent bank may have. If this does not occur, however, respondent banks should react promptly when faced with a termination notice. Initiating a detailed dialogue with the correspondent bank about the specific issues or reasons for the termination will assist the respondent bank in developing an action plan that can remediate the identified deficiencies in a timely manner. If the correspondent bank does not find the remedial actions satisfactory and the termination is unavoidable, the respondent bank should consider asking for an extension that may allow for additional time to find an alternative correspondent bank relationship.

In summary, ongoing communication of your efforts to keep up with evolving regulatory, international, and correspondent bank AML/CFT program expectations will improve your ability to meet expectations and maintain CBRs.

Example: Handling a Termination Notice

In one country, a respondent bank's practice showed the value of taking immediate action after being notified by the global bank of its intention to terminate the relationship. The respondent bank immediately insisted on a person-to-person meeting with senior management of its correspondent bank at its U.K. headquarters; the respondent succeeded in extending the original termination notice of 30 days to 1 year. They also agreed on a corrective action plan. While the ultimate reasons for the correspondent bank's decision to extend the period cannot be verified, the respondents mentioned that they would consider taking the case to court, pointing out the low risk of its customer base (predominantly pensioners receiving state pensions from U.K. government). Prompt action and the threat of negative publicity may have played a role in that decision, too.

Source: The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.

Chapter 5
AML/CFT Program Maturity Framework Self-assessment

As part of a continuous improvement process, banks are to periodically assess their AML/CFT program's maturity level. This will enable banks to identify potential weaknesses or deficiencies in the existing AML/CFT program and assist in the development of a corrective action plan to achieve the next maturity level. It will also be useful to share such assessments with relevant parties, including correspondent banks, banks supervisors, and so forth, and to communicate your status and plans for improvements in a proactive fashion.

Given the evolving landscape of AML/CFT compliance, components of an AML/CFT program can possess differing levels of effectiveness/maturity as compared with best practices. In addition to changes in compliance standards, impacts to levels of program maturity may include changes in senior and middle management; financial crime leadership and core expertise; meaningful changes in business strategies; changes in customer base; evolution of regulatory expectations; as well as a board's lack of support and tone at the top. Each of these and other factors could affect a point-in-time assessment of an AML/CFT program's maturity.

The matrix that follows presents a maturity framework to help guide emerging-market banks in self-assessing their AML/CFT program. This framework includes essential AML/CFT component parts and supports assessing where a program stands. The framework presents four levels of maturity (**basic**, **emerging**, **developed**, and **advanced**) and includes general descriptors of what each maturity level indicates.

The goal of this is to assist banks in assessing not only their overall AML program maturity but also the individual maturity levels of the core components of sound AML/CFT risk management. Banks should go through each component of this framework, from governance to internal and external audit, and determine which descriptor and level fits their institution best. This self-assessment is not a certification or validation but is intended to support banks in their ongoing efforts to identify areas of strength and areas in need of enhancement. This process can also be incorporated as part of an enterprise wide continuing improvement processes.

IFC has also developed a software based detailed diagnostic tool designed to measure an AML/CFT program's maturity. That tool is closely aligned with the maturity matrix that follows. Emerging-market banks should consider reaching out to the IFC regarding the use of this tool to enhance assessment of their own AML/CFT risk frameworks.

Component	Basic	Emerging	Developed	Advanced
Governance	The board has not approved an AML/CFT governance structure. Roles and responsibilities related to AML/CFT are not clearly articulated and defined. ML/FT risk management is not integrated into the three lines of defense (business units, AML/CFT compliance function, and internal audit), and most of AML/CFT compliance responsibilities may be carried out by business units.	The board has not approved an AML/CFT governance structure. Roles and responsibilities have been defined but for a limited number of ML/FT risks. ML/FT risk management is not integrated into three lines of defense (for example, the internal audit function does not exist and/or business units are not involved in ML/FT risk management).	The bank has a formal AML/CFT governance structure that was approved by the board. Although these governance arrangements have not been clearly communicated throughout the institution, ML/FT risks are managed by all three lines of defense.	The bank has a formal AML/CFT governance structure that was approved by the board. Clearly defined roles and responsibilities related to AML/CFT have been communicated throughout the institution and are well understood by all relevant employees. ML/FT risk management is integrated into three lines of defense.
	The board has not defined the bank's risk tolerance.	The board has defined the bank's risk tolerance but has not communicated it across the institution.	The board has defined the bank's risk tolerance and ensured that it is understood by all relevant personnel and that each business unit has defined its risk appetite clearly.	The board has defined the bank's risk tolerance and ensured that it is understood by all relevant personnel and that each business unit has defined its risk appetite clearly. The bank's and business units' risk tolerance statements are reviewed and approved on a regular basis.
	The board is not actively involved in the AML/CFT risk prevention and does not typically receive the results of the risk assessment and any measures taken by the bank to manage the identified risks.	There is board involvement in the AML/CFT risk prevention, but it is rather sporadic and limited. Reports on the results of the risk assessment and any measures taken by the bank occur less frequently than once a year.	The board receives reports on all major AML/CFT compliance matters once a year and earlier if material issues arise. The bank typically has a senior management committee responsible for AML/CFT compliance that also receives reports on all major AML/CFT compliance matters.	The board receives reports on all major AML/CFT compliance matters multiple times a year (for example, quarterly) and earlier if material issues arise. The bank typically has a senior management committee and subcommittees responsible for AML/CFT compliance that also receive(s) reports on all major AML/CFT compliance matters.
	There is no appointed AML/CFT officer.	There is an appointed AML/CFT officer, but his/her responsibilities are not distinct from business-line responsibilities and other executive functions, such as CFO, CEO, or chief auditor and/or AML/CFT officer, and he/she does not have AML/CFT authority across the entire institution.	There is an appointed AML/CFT officer who is responsible for the AML/CFT function across the entire institution and has sufficient authority and seniority within the bank to be able to influence decisions related to AML/CFT. The AML/CFT officer has direct access to the board.	There is an appointed AML/CFT officer who is responsible for the AML/CFT function across the entire institution. However, the officer reports directly to the CEO or CFO or other similar function and has no direct access to the board.

Component	Basic	Emerging	Developed	Advanced
Risk identification, assessment and mitigation	The bank has not conducted an AML/CFT risk assessment at the enterprise wide level; AML/CFT risk assessments were performed in selected business units or branches only and did not cover all the relevant inherent risk components (customer base, products/services, delivery channels, jurisdictions, or other qualitative factors such as recent enforcement actions).	The bank conducts an enterprise wide AML/CFT risk assessment that includes (i) only a few of the relevant inherent risk components (customer base, products/services, delivery channels, jurisdictions, or other qualitative factors, such as recent enforcement actions) applied inconsistently and sporadically across some of the business units; and (ii) an assessment of only a few of the internal controls the bank has in place.	The bank conducts an enterprise wide AML/CFT risk assessment that includes (i) some of the relevant inherent risk components (customer base, products/services, delivery channels, jurisdictions, or other qualitative factors, such as recent enforcement actions) applied inconsistently across all in-scope business units, divisions, and legal entities; and (ii) an assessment of most of the internal controls the bank has in place.	The bank's enterprise wide AML/CFT risk assessment includes (i) all the relevant inherent risk components (customer base, products/services, delivery channels, jurisdictions, and other qualitative factors, such as recent enforcement actions) consistently applied across all in-scope business units, divisions and legal entities; and (ii) an assessment of all the internal controls the bank has in place.
	The bank does not have a process for risk rating customers, products and services, and countries it does business with.	The bank is currently using customer, products and services, and country risk rating methodologies; however, this requirement is not documented in the bank's policies and procedures. The bank does not typically review and update these methodologies.	The bank has a process for risk rating customers, products and services, and countries it does business with. The bank's policies and procedures do not specify the requirement to review and update these methodologies on a regular basis; however, they are typically reviewed and updated every 2–3 years.	The bank has a process for risk rating customers, products and services, and countries it does business with. These methodologies are reviewed and updated on a regular basis (for example, annually). This requirement is documented in the bank's policies and procedures.
	The bank has not conducted an enterprise wide AML/CFT risk assessment. The bank conducts only business-line assessments and has only partially completed them. The risk assessment methodology is mainly based on internal information, qualitative in nature, and includes a limited number of factors. It is either poorly documented or not documented and is not typically approved by senior management.	The bank conducts an enterprise wide AML/CFT risk assessment every 24–36 months. The risk assessment methodology is mainly based on internal information, includes both qualitative and quantitative factors, but the number of quantitative factors is limited. Although the risk assessment methodology is documented, senior management does not typically approve it.	The bank conducts an enterprise wide AML/CFT risk assessment every 12–18 months. The risk assessment methodology is based on internal information, such as operational and transactional data produced by the bank, as well as external information, such as country reports from various international organizations and national risk assessments and includes both qualitative and quantitative elements (for example, volume and value of transactions). It is clearly documented and reviewed and approved by senior management every 2–3 years.	The bank conducts an enterprise wide AML/CFT risk assessment every 12–18 months. A more-frequent refresh is performed if new or emerging risks that significantly change the bank's risk profile are identified. The risk-assessment methodology is based on internal information, such as operational and transactional data produced by the bank, as well as external information, such as country reports from various international organizations and national risk assessments and includes both qualitative and quantitative elements (for example, volume and value of transactions). It is clearly documented and approved by senior management on a regular basis (at least annually or on a more-frequent basis, if applicable).

Component	Basic	Emerging	Developed	Advanced
Policies and procedures	The bank does not have a documented enterprise wide AML/CFT policy. Informal policy is inconsistently applied across business units.	The bank has a documented enterprise wide AML/CFT policy that covers only some of the main AML/CFT compliance areas; significant gaps exist. The policy is approved by the board less frequently than annually and does not explicitly state such a requirement.	The bank has a documented enterprise wide AML/CFT policy that covers most of the main AML/CFT compliance areas; insignificant gaps exist. The policy is approved by the board annually but does not explicitly state such a requirement.	The bank has a documented enterprise wide AML/CFT policy that covers all main AML/CFT compliance areas (such as appointment of an AML/CFT officer, risk assessment, policies and procedures, CDD, transaction monitoring). The policy is approved by the board at least annually, and the policy explicitly states such a requirement.
	The bank either does not have line of business (LOB)-level AML/CFT procedures, or the procedures have significant coverage gaps, are not always easily available to all applicable employees, and are not updated on an ongoing basis. The procedures are not reviewed and approved by the AML/CFT compliance function.	Detailed LOB-level AML/CFT procedures are in place, but coverage gaps exist. The procedures are updated infrequently, and this requirement is not explicitly stated in the procedures. The procedures are not always easily available to all applicable employees. The procedures are not reviewed and approved by the AML/CFT compliance function.	Detailed LOB-level AML/CFT procedures exist, cover main AML/CFT compliance areas (such as CDD, EDD, transaction monitoring, record retention, training), and are easily available to all employees. The procedures are periodically updated, but this requirement is not explicitly stated in the procedures. The procedures are not reviewed and approved by the AML/CFT compliance function.	Detailed LOB-level AML/CFT procedures exist and cover main AML/CFT compliance areas (such as CDD, EDD, transaction monitoring, record retention, and training). The procedures are updated on an annual basis, and this requirement is explicitly stated in the procedures. The procedures are reviewed and approved by the AML/CFT compliance function and are easily available to all employees.
	The bank's AML/CFT policies and procedures do not address prohibited relationships.	The bank's AML/CFT policies and procedures address prohibited relationships, but they do not explicitly prohibit the relationships, accounts, and transactions expected to be prohibited by international standards (for example, anonymous accounts or accounts in obviously fictitious names, shell banks, and designated persons and entities).	The bank's AML/CFT policies and procedures explicitly prohibit some of the relationships, accounts, and transactions expected to be prohibited by international standards (for example, anonymous accounts or accounts in obviously fictitious names, shell banks, and designated persons and entities).	The bank's AML/CFT policies and procedures explicitly prohibit relationships, accounts, and transactions expected to be prohibited by international standards (for example, anonymous accounts or accounts in obviously fictitious names, shell banks, and designated persons and entities).

Component	Basic	Emerging	Developed	Advanced
	The bank's AML/CFT policies and procedures do not follow a risk-based approach.	Some AML/CFT policies and procedures follow a risk-based approach; this approach is used in some applicable areas (for example, at customer onboarding or ongoing due diligence).	The bank's AML/CFT policies and procedures follow a risk-based approach and are designed to adequately mitigate the inherent risks identified by the risk assessment. The risk-based approach is used in all applicable areas (for example, at customer onboarding, ongoing due diligence, and transaction monitoring).	The bank's AML/CFT policies and procedures follow a risk-based approach and are designed to adequately mitigate the inherent risks identified by the risk assessment. The risk-based approach is formally documented in the policies and procedures and is used in all applicable areas (for example, at customer onboarding, ongoing due diligence, and transaction monitoring). The policies and procedures are updated on a regular basis to address newly identified inherent risks.
Customer identification and due diligence	The bank generally identifies and verifies customers but does not have a formal process for identifying and verifying beneficial owners, authorized signatories, and key controllers. The bank's policies and procedures do not specify the time frame within which required information must be collected and how to handle exceptions. Beyond customer identification and verification, the bank generally does not collect any additional due diligence.	The bank has a process for (i) identifying and verifying customers and beneficial owners; and (ii) conducting customer due diligence/enhanced due diligence (CDD/EDD) on its customers that includes only a few of the elements expected to be collected by international standards (for example, purpose and nature of relationship, product usage, expected activity, and source of funds). The bank's policies and procedures do not indicate whether ultimate beneficial owners, authorized signatories, and key controllers are required to be identified and verified. Additionally, the bank's policies and procedures do not specify the time frame within which required information must be collected and how to handle exceptions.	The bank has a process for (i) identifying and verifying customers, beneficial owners, including ultimate beneficial owners, authorized signatories, and key controllers; and (ii) conducting CDD/EDD on its customers that includes most of the elements expected to be collected by international standards (for example, purpose and nature of relationship, product usage, expected activity, and source of funds). The required information is collected and verified at onboarding or within a reasonable time (for example, 60–90 days). The bank will open the account, allowing the customer to transact, but such transactions will be monitored by the AML/CFT compliance department until the verification process is complete. If the bank cannot obtain and verify the customer's identifying information within 60–90 days, it will close the account and consider filing a suspicious-transaction report. These requirements are formally documented in policies and procedures.	The bank has a process for (i) identifying and verifying customers, beneficial owners, including ultimate beneficial owners, authorized signatories, and key controllers; and (ii) conducting CDD/EDD on its customers that includes all the elements expected to be collected by international standards (for example, purpose and nature of relationship, product usage, expected activity, and source of funds). The required information is collected and verified at onboarding or shortly thereafter (for example, within 30 days). The bank will not open the account until such process is complete and will consider filing a suspicious-transaction report in relation to the customer if information cannot be obtained and/or verified. These requirements are formally documented in policies and procedures, and all exceptions are closely monitored by the AML/CFT compliance department.

Component	Basic	Emerging	Developed	Advanced
	The bank does not have a formal enterprise wide CRR process. CRR has been performed in selected business units or branches only and does not cover all the relevant risk factors (for example, geography, product usage, industry, legal entity type, and screening results).	The bank conducts CRR that includes only a few of the relevant risk factors (for example, geography, product usage, industry, legal entity type, and screening results); significant gaps exist. This requirement is poorly documented in the bank's policies and procedures.	The bank conducts CRR that includes most of the relevant risk factors (for example, geography, product usage, industry, legal entity type, and screening results); insignificant gaps exist.	The bank conducts CRR that includes all the relevant risk factors (for example, geography, product usage, industry, legal entity type, and screening results).
	The bank does not have a formal process for reviewing and updating customer information. Informal review, if performed, is inconsistently applied across business units.	The bank has a process for conducting periodic reviews of high-risk customers only. Medium- and lower-risk customers are not typically reviewed.	The bank has a process for periodically updating customer information. All customers (higher-, medium-, and lower-risk) are reviewed based on a trigger event. The policies and procedures clearly document what information needs to be updated and how this process should be carried out. If the bank cannot collect the required information within a prescribed time frame (for example, 30–60 days), it will consider terminating the relationship.	The bank has a process for periodically updating customer information. Higher-risk customers are reviewed every year. Medium- and lower-risk customers are reviewed every 2–5 years or based on a trigger event. The policies and procedures clearly document what information needs to be updated and how this process should be carried out. If the bank cannot collect the required information within a prescribed time frame (for example, 30–60 days), it will consider terminating the relationship.
	The bank generally conducts screening at customer onboarding and sporadically after that. The screening process is manual and may not include PEP screening. This process is not formally documented in the bank's policies and procedures and is not carried out consistently.	The bank typically conducts terrorist/ sanctions, negative news, and PEP screening at customer onboarding and based on a trigger event. The screening process is manual. The bank's policies and procedures do not clearly explain which customers and related parties are required to be screened and how this process should be carried out.	The bank conducts terrorist/sanctions, negative news, and PEP screening at customer onboarding, during periodic review, and based on a trigger event. The screening process is a combination of automated and manual. Potential matches are reviewed and escalated in a timely manner. The bank's policies and procedures clearly explain which customers and related parties are required to be screened and how this process should be carried out.	The bank conducts terrorist/sanctions, negative news, and PEP screening at customer onboarding and on a frequent basis thereafter (for example, daily or weekly). The screening process is fully automated. Potential matches are promptly reviewed and escalated. The bank's policies and procedures clearly explain which customers and related parties are required to be screened and how this process should be carried out.

Component	Basic	Emerging	Developed	Advanced
Transaction monitoring	The bank does not have a documented process to perform transaction monitoring to identify unusual/ suspicious transactions and customers. AML/CFT compliance periodically conducts informal manual review of transactions, but such review is sporadic and limited.	The bank performs transaction monitoring to identify unusual/ suspicious transactions and customers. The method used by the bank is manual. This requirement is poorly documented in the bank's policies and procedures.	The bank performs transaction monitoring to identify unusual/ suspicious transactions and customers. The method used by the bank is a combination of automated and manual. The bank's policies and procedures address this requirement.	The bank performs transaction monitoring to identify unusual/ suspicious transactions and customers using an automated transaction monitoring tool. The bank's policies and procedures address this requirement.
	The bank does not have a formal process for reviewing, investigating, and escalating unusual/ potentially suspicious activity. AML/CFT compliance periodically reviews alerts and employee referrals, but such review is sporadic and limited.	All unusual/potentially suspicious activity that has been identified by the transaction monitoring solution or through other means, such as employee referrals, is reviewed and investigated. No review of activity determined to be suspicious is performed by a senior person. These requirements are poorly documented in the bank's policies and procedures.	All unusual/potentially suspicious activity that has been identified by the transaction monitoring solution or through other means, such as employee referrals, is reviewed, investigated, and, where applicable, escalated to senior personnel. A sample of activity determined to be suspicious is reviewed by a senior person. The bank's policies and procedures address these requirements, but insignificant gaps exist.	All unusual/potentially suspicious activity that has been identified by the transaction monitoring solution or through other means, such as employee referrals, is reviewed, investigated, and, if applicable, escalated within a prescribed time frame (for example, 30 days). All activity determined to be suspicious is reviewed by a senior person (and/or a suspicious-transaction report review committee). These requirements are clearly documented in the bank's policies and procedures.
	The bank has not performed an analysis to identify the applicable red flag behavior that should be monitored.	The bank has identified the applicable red flag behavior that should be monitored. Only a few of the identified red flags are tracked by the automated transaction monitoring system or manual processes. The bank does not typically update the list of red flags.	The bank has identified the applicable red flag behavior that should be monitored. Although the procedures do not specify the requirement to update these red flags periodically, they are typically reviewed every 2–3 years. Most red flags are currently tracked by the automated transaction monitoring system or manual processes.	The bank has identified the applicable red flag behavior that should be monitored. These red flags are periodically reviewed (at least annually). The bank mapped the red flags to the rules available in its transaction monitoring system; for the red flags not currently tracked by the automated transaction monitoring system, the bank has manual processes. The bank's policies and procedures specify such a requirement.

Component	Basic	Emerging	Developed	Advanced
	The bank does not use a transaction monitoring system.	The bank uses a transaction monitoring system. The rules in the transaction monitoring system are generic and do not establish different thresholds for different customer segments and customers of different risk levels. The rules are not reviewed/approved on a regular basis.	The bank uses a transaction monitoring system. The rules in the transaction monitoring system are tuned based on the actual customer transactional activity. There are different thresholds applied to different customer segments and customers of different risk levels. The bank's policies and procedures do not specify the requirement to periodically review the rules; however, they are typically reviewed and approved every 2–3 years.	The bank uses a transaction monitoring system. The rules in the transaction monitoring system are fine-tuned based on the actual customer transactional activity. There are different thresholds applied to different customer segments and customers of different risk levels. The rules are reviewed on a regular basis (for example, at least once a year) to determine whether tuning is necessary and are annually approved by the chief AML/CFT officer. These requirements are documented in the bank's policies and procedures.
Reporting	Management reporting is sporadic and limited; there is limited involvement from management in the prevention of ML/FT risks.	The bank has management reporting in place that covers only a few of the relevant AML/CFT areas (for example, risk assessment, high-risk customers, suspicious transaction reports, transaction monitoring alerts, and customers with outstanding EDD/CDD/identification verifications). The reporting typically occurs once a year. These requirements are poorly documented in the bank's policies and procedures.	The bank has regular management reporting in place covering most of the relevant AML/CFT areas (for example, risk assessment, high-risk customers, suspicious transaction reports, transaction monitoring alerts, and customers with outstanding EDD/CDD/identification verifications). The reports are made available to all relevant stakeholders from the board of directors and senior management to operational management once a year. These requirements are documented in the bank's policies and procedures. The bank does not have formal processes in place to track special projects related to AML/CFT compliance.	The bank has regular management reporting in place covering all the relevant AML/CFT areas (for example, risk assessment, high-risk customers, suspicious transaction reports, transaction monitoring alerts, and customers with outstanding EDD/CDD/identification verifications). The reports are made available to all relevant stakeholders from the board of directors and senior management to operational management on a frequent basis (for example, monthly or quarterly). The bank has formal processes in place to track, monitor, and report on special projects related to AML/CFT compliance (for example, elimination of backlog or KYC remediation). These requirements are documented in the bank's policies and procedures.

Component	Basic	Emerging	Developed	Advanced
	The bank's policies and procedures do not outline the process for reporting suspicious/ unusual transactions to the respective supervisory body. Reporting of STRs is sporadic, and STRs are not reviewed by a senior compliance person.	Identified unusual/ suspicious transactions are typically reported to the respective supervisory body but not always in a timely manner. Such process and timing requirements are poorly documented in the bank's policies and procedures. STRs are not reviewed by a senior compliance person.	All identified unusual/ suspicious transactions are reported in a timely manner to the respective supervisory body. The bank includes all relevant details of the suspicious/ unusual transactions, including the background and purpose of the transaction, who was involved, when and where it occurred, and what products and services were involved. The bank's policies and procedures address such reporting process and timing requirements, but insignificant gaps exist. Only a sample of STRs is reviewed by a senior compliance person.	All identified unusual/ suspicious transactions are reported in a timely manner to the respective supervisory body. The bank includes all relevant details of the suspicious/ unusual transactions, including the background and purpose of the transaction, who was involved, when and where it occurred, and what products and services were involved. The bank's policies and procedures address such reporting process and timing requirements. All STRs are reviewed by a senior compliance person.
	The bank's policies and procedures do not address the process for identifying, aggregating, and reporting cash (currency) transactions to the respective supervisory body; informal reporting is sporadic and not always timely. If reporting occurs, cash aggregation process and cash (currency) reports are not subject to quality control.	Cash (currency) reports are typically reported to the respective supervisory body but not always in a timely manner. Such process and timing requirements are poorly documented in the bank's policies and procedures. Cash aggregation process and cash (currency) reports are not subject to quality control.	The bank identifies, aggregates, and reports cash (currency) transactions to the respective supervisory body in a timely manner. The bank's policies and procedures address such reporting process and timing requirements; however, cash aggregation process and cash (currency) reports are not subject to quality control.	The bank identifies, aggregates, and reports cash (currency) transactions to the respective supervisory body in a timely manner. Cash aggregation process and cash (currency) reports are subject to quality control. The bank's policies and procedures address such reporting process and timing requirements.
Communication and training	Information sharing between departments rarely occurs. This process is not documented in the bank's policies and procedures.	Information sharing between departments occurs but not always in a consistent and timely manner. This process is poorly documented in the bank's policies procedures.	Information sharing between departments occurs on a regular basis, and the AML/ CFT compliance staff typically receive relevant information from other departments in a timely manner. Most of these requirements are documented in the bank's policies and procedures, but insignificant gaps exist.	The information sharing process in place allows relevant information to flow across the entire institution. The AML/CFT compliance staff receive relevant information from other departments in a timely manner. This requirement is documented in the bank's policies and procedures. The importance of sharing relevant information with the AML/CFT compliance function is emphasized by the board and senior management.

Component	Basic	Emerging	Developed	Advanced
	The bank does not have mandatory AML/CFT training in place.	The bank provides generic AML/CFT training that is not targeted to specific roles and responsibilities. There is no requirement to pass a test at the end of the training with a minimum completion score. Training is provided when personnel are hired; there is no mandatory training on an ongoing basis. The board, third parties, and contractors/ consultants are not required to take training.	The bank provides mandatory AML/CFT training that is targeted to specific roles and responsibilities when personnel are hired and on an annual basis. All personnel are required to pass a test at the end of the training with a minimum completion score. The follow-up steps in cases in which an employee fails the test (for example, requirement to retake the test or temporary license revoked for agents) are not documented in the bank's policies and procedures and are not always carried out. All relevant personnel receive mandatory training, including the board, third parties, and contractors/consultants.	The bank provides mandatory AML/CFT training that is targeted to specific roles and responsibilities when personnel are hired and on an annual basis. All personnel are required to pass a test at the end of the training with a minimum completion score. There are follow-up steps in cases in which an employee fails the test (for example, requirement to retake the test or temporary license revoked for agents), which are clearly documented in the bank's policies and procedures. Mandatory training is typically not provided to third parties or contractors/ consultants.
	Adherence to AML/CFT compliance requirements is not incorporated into performance evaluation of appropriate bank personnel; no disciplinary actions are taken in case of noncompliance.	Adherence to AML/CFT compliance requirements has not been embraced throughout the institution and is incorporated into performance evaluations of only some of the personnel; significant gaps exit. Disciplinary actions are taken occasionally, and this process has not been formalized.	Adherence to AML/CFT compliance requirements is formally incorporated into performance evaluations of most of the appropriate personnel. Disciplinary actions up to and including termination are taken promptly if an employee is found not to comply with AML/CFT requirements.	Adherence to AML/CFT compliance requirements is formally incorporated into performance evaluations of all appropriate personnel. Disciplinary actions up to and including termination are taken promptly if an employee is found not to comply with AML/CFT requirements.
	AML/CFT compliance function is not fully developed. Most of AML/CFT compliance responsibilities are carried out by business units' personnel who are not independent. Significant lack of resources causes frequent backlogs and affects the bank's ability to comply with its statutory requirements.	AML/CFT compliance function exists, but some employees within this function are not fully independent and perform responsibilities that conflict with their compliance responsibilities (for example, involved in the internal audit function). There is a lack of resources and no quality assurance process in place.	AML/CFT compliance function exists, and employees within this function are independent and have sufficient resources. AML/CFT compliance function conducts periodic compliance testing of their processes and controls, but there is no reporting on their findings, and this is not formally documented in their policies and procedures.	AML/CFT compliance function exists and has sufficient resources (adequate number of employees and access to necessary systems, information, and bank personnel). Employees within the AML/CFT compliance function are independent (that is, not in a position where there is conflict of interest between their compliance responsibilities and any other responsibilities). AML/CFT compliance function conducts periodic compliance testing of their processes and controls, reports on their findings, and this is incorporated in their policies and procedures.

Component	Basic	Emerging	Developed	Advanced
Continuous improvement and testing	The bank does not have an AML/CFT compliance testing/quality assurance process in place.	The bank has AML/CFT compliance testing/ quality assurance process in place, but it includes only a few of the relevant AML/CFT processes (for example, CDD, STR reporting, cash transaction reporting, and training) and they occur infrequently. Testing/ quality assurance process requirements are poorly documented in the bank's policies and procedures.	The bank's AML/CFT compliance department tests/conducts quality assurance of some of the relevant AML/CFT processes (for example, CDD, STR reporting, cash transaction reporting, and training). Testing/quality assurance is typically performed annually, and such requirement is documented in the bank's policies and procedures.	The bank's AML/CFT compliance department tests/conducts quality assurance of all the relevant AML/CFT processes (for example, CDD, STR reporting, cash transaction reporting, and training). Testing/quality assurance is performed on a frequent basis (monthly or quarterly), and such requirement is documented in the bank's policies and procedures.
	The bank's AML/CFT compliance function does not perform testing of the AML/CFT methodologies used by the bank (for example, CRR, product risk rating, and country risk rating).	The bank's AML/CFT compliance function performs testing of some of the AML/CFT methodologies used by the bank (for example, CRR, product risk rating, and country risk rating). This process is sporadic and limited. A technical validation of models is typically not performed as part of this testing or is performed on an infrequent and limited basis. This requirement and frequency of testing are not documented in the bank's policies and procedures.	The bank's AML/CFT compliance function periodically performs testing of all the AML/ CFT methodologies used by the bank (for example, CRR, product risk rating, and country risk rating). As part of this testing, the bank typically performs a technical validation of models, including data management, back-testing, and testing for false positive alerts. These requirements are documented in the bank's policies and procedures but some gaps exist (for example, the frequency of testing is not addressed).	The bank's AML/CFT compliance function performs testing of all the AML/CFT methodologies used by the bank (for example, customer risk rating, product risk rating, country risk rating) on an annual basis. As part of this testing, the bank performs a technical validation of models including data management, back-testing, and testing for false-positive alerts. These requirements are documented in the bank's policies and procedures.
Internal and external audit	The bank does not have an internal audit function.	The bank has an internal audit function reporting to the CEO or equivalent. It lacks independence and resources to adequately perform its responsibilities with objectivity. The internal audit department's recommendations are rarely implemented by the bank.	The bank has an internal audit function reporting to the CEO or equivalent but has sufficient authority to perform most of their responsibilities with objectivity. Some of their recommendations are implemented by appropriate departments in a timely manner.	The bank has an internal audit function reporting directly to the board or equivalent senior management committee. The internal audit department is independent and has sufficient authority to perform their responsibilities with objectivity. All their recommendations are implemented by appropriate departments in a timely manner.

Component	Basic	Emerging	Developed	Advanced
	The bank rarely conducts an independent audit/ testing of the AML/CFT program. The bank's policies and procedures do not address this requirement.	The bank's AML/CFT program is subject to an independent internal audit but not on a regular basis. The bank does not engage external auditors to assess the AML/CFT program. Audit scope has significant gaps. Audit results are typically shared with the AML/CFT officer only and are not shared with the board and senior management. These requirements are not clearly outlined in the bank's policies and procedures.	The bank's AML/CFT program is subject to an independent audit on a regular basis (for example, every 12–18 months). Independent audit is typically carried out by internal auditors but occasionally by external auditors. Audit scope is typically comprehensive, but some gaps may exist. Audit results are shared with the board, senior management, and the AML/CFT officer. Where deficiencies are identified, a formal action plan is developed, but there is no formal tracking of the progress on the action plan. These requirements are documented in the bank's policies and procedures.	The bank's AML/CFT program is subject to a comprehensive independent audit by internal and/or external auditors on an annual basis. Audit results are shared with the board, senior management, and the AML/CFT officer. Where deficiencies are identified, a formal action plan is developed, and the progress on the action plan is reported to senior management on a regular basis. These requirements are documented in the bank's policies and procedures.

Chapter 6
Conclusion

In support of the IFC's mission and their long-standing history of developing initiatives in support of the marketplace, the goal of the development of the GPN is to provide best-practice guidance and practical solutions to help emerging-market respondent banks maintain and obtain, if necessary, correspondent bank relationships. In addition to the GPN, the IFC has developed and is piloting a software-based diagnostic tool to assist IFC client banks and partners in assessing the maturity of their AML/CFT program. The GPN and Diagnostic Tool present a way forward for respondent banks to counter de-risking issues and challenges.

The GPN outlines the business case for investing in AML/CFT risk management along with international expectations, standards, and processes that can help respondent banks understand the critical processes, including AML/CFT, proper governance structure and operation, key AML/CFT internal controls, enhanced automated risk management and suspicious-activity monitoring in order to stay ahead of correspondent bank expectations and requests for information. Applying these good practices can also potentially minimize bank supervisory sanction/penalty exposures and reduce long term compliance costs. Following the guidance can provide an opportunity for banks in emerging markets to identify weaknesses or deficiencies in their AML/CFT program in a timely manner and proactively address such issues before they affect any correspondent bank relationships.

The GPN and Diagnostic Tool are designed to:

1. *Provide international and industry good practices on how to approach these challenges from the perspective of developing and implementing an adequate risk management framework, including an AML/CFT compliance risk management program and program oversight. This information can help to identify, measure, monitor, manage, and report concerns associated with bank- and jurisdiction-related AML/CFT risks. Specifically, the Diagnostic Tool is a self-assessment tool designed to evaluate the state of the AML/CFT program maturity and details four maturity levels for 11 components of an AML/CFT program.*
2. *Assist in the understanding of the correspondent bank perspective to help respondent banks rise to the expectations and quickly and efficiently address issues or questions arising from risk, profitability, and perceptions of jurisdictional risk.*
3. *Introduce the value of third-party testing to independently document the effectiveness of AML/CFT controls. This testing activity can help respondent banks identify possible issues and develop corrective action plans.*

Although the GPN cannot address all individual bank issues (for example, the revenue/profitability, risk appetite, and correspondent bank access to necessary information) it does provide a framework that can facilitate and potentially alleviate correspondent bank issues before, during, or after any concerns arise.

In closing, we have identified a number of key success factors for respondent banks. As such, there are multiple critical actions and factors that need to be considered when leveraging the GPN and the Diagnostic Tool to greatly improve a respondent bank's opportunity for CBR success; they include:

a. *Document active board and senior management oversight and commitment to AML/CFT risk management and compliance, including investments*

in resources (staffing and technology) to adequately support the compliance function;

b. *Design, develop, and implement a risk assessment and CRR process to identify risk exposures and determine which applicable controls are needed to mitigate the corporate and individual customer risks;*

c. *Design, implement, and ultimately independently test a robust AML/CFT program to demonstrate its effectiveness to correspondent banks;*

d. *Leverage technology and industry information-sharing services such as KYC utilities, LEIs, and advanced software for STR to amplify the effectiveness of the respondent bank's AML/CFT program elements;*

e. *Work with FIUs, local regulators, correspondent banks, peer banks, and international organizations to keep up with expectations and requirements, and to facilitate information sharing to support the mission of AML/CFT and risk management of all parties involved; and*

f. *Use third-party resources to verify the effectiveness of AML/CFT programs to provide an independent assessment of their effectiveness.*

This GPN and Diagnostic Tool were designed to assist and support respondent banks, particularly those in emerging markets, to effectively address the substantial environmental challenges in obtaining and maintaining correspondent relationships during this time of de-risking. Using the information provided and acting to address gaps should provide you with the means to protect your bank as much as possible from external impacts affecting your correspondent bank relationships and provide a competitive advantage in serving your local customers.

Annex 1: Initiatives Undertaken by International Institutions and Systemic Banks to Address De-risking

Listed here are some of the initiatives on correspondent banking undertaken by the international community that may be of interest.

The Financial Stability Board

In November 2015, the Financial Stability Board (FSB) presented to the G20 leaders an action plan consisting of the following four elements:

- *Further examining the dimensions and implications of the issue;*
- *Clarifying regulatory expectations, as a matter of priority, including more guidance by the Financial Action Task Force (FATF);*
- *Increasing domestic capacity-building in jurisdictions that are home to affected respondent banks; and*
- *Strengthening tools for due diligence by correspondent banks.*

In March 2016, the FSB established the Correspondent Banking Coordination Group (CBCG) to coordinate the implementation of the action plan.[77]

In March 2018, the FSB issued a publication providing recommendations to improve the accessibility of banking services to remittance service providers.[78]

The Financial Action Task Force

In October 2016, guidance on correspondent banking services[79] to clarify expectations for correspondent institutions when dealing with respondents was published. In its publication, the FATF stated: "de-risking may drive financial transactions into less/non-regulated channels, reducing transparency of financial flows and creating financial exclusion, thereby increasing exposure to money laundering and terrorist financing (ML/TF) risks." To provide additional clarification on customer due diligence for correspondent banking relationships, it stated: "the FATF recommendations do not require financial institutions to conduct customer due diligence on the customers of their customers (i.e., each individual customer)."

In November 2017, FATF published guidance on anti-money laundering/countering the financing of terrorism (AML/CFT) measures and financial inclusion, with a supplement on customer due diligence that encourages financial institutions to design AML/CFT measures that do not hinder financial inclusion. The revised guidance reinforces the risk-based approach as an underlying principle of AML/CFT programs.[80]

---

77 FSB. 2015. Report to the G20 on Actions Taken to Assess and Address the Decline in Correspondent Banking.
78 FSB. 2018. Stocktake of Remittance Service Providers' Access to Banking Services.
79 FATF. 2016. Correspondent Banking Services.
80 FATF. 2017. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.

The Basel Committee on Banking Supervision

In January 2014, Sound Management of Risks related to Money Laundering and Financing of Terrorism Guidelines, which included an annex on correspondent banking (including money laundering/financing of terrorism risk assessments and customer due diligence requirements in correspondent banking) was published.

In June 2017, the Basel Committee on Banking Supervision (BCBS) released an updated version of these guidelines with final revisions to Annex 2: Correspondent Banking and Annex 4: General Guide to Account Opening.[81]

Committee on Payments and Market Infrastructures

In July 2016, Committee on Payment and Market Infrastructures (CPMI) issued a report in which it recommended that banks involved in correspondent banking consider the use of the legal entity identifier (LEI) in payment messages as a means of identification that should be provided in know your client (KYC) utilities and information-sharing arrangements. The LEI's widespread use could facilitate and increase the effectiveness of AML/CFT screening by reducing the number of false-positive alert when screening names and addresses that only partially match the data of a given entity.[82]

The Wolfsberg Group

In February 2018, the Wolfsberg Group published the Correspondent Banking Due Diligence Questionnaire, which is intended to support a more standardized collection of information on respondent banks and strengthen tools for due diligence by correspondent banks. The questionnaire is believed to be one of the industry initiatives that will help address the decline in the number of correspondent banking relationships.

The Monetary Authority of Singapore

Per the Monetary Authority of Singapore, KYC is one of the most complex processes in the financial industry because it is costly, labor intensive, and redundant. As such, the Monetary Authority of Singapore is working closely with local and foreign banks to explore a banking KYC shared-services utility to streamline KYC that can promote the maintenance of CBRs. This KYC utility will centralize processes such as:

1. *Leveraging on MyInfo (a single platform containing personal data submitted to and verified by the government) for customer identification and verification;*
2. *Collecting and validating KYC documents; and*
3. *Screening against sanctions and blacklists.*

The banking KYC utility is expected to harmonize and enhance KYC checks across the industry and improve the quality of risk management while reducing cost and time taken.[83]

Thomson Reuters KYC

In July 2016, three South African banks (Barclays Africa, Rand Merchant Bank, and Standard Bank of South Africa) partnered with Thomson Reuters to design and launch the South African KYC managed service.

This KYC managed service provides the following benefits:

- *The cost of a KYC managed service is shared across multiple banks.*
- *Customer documentation can be kept in one central place.*
- *Duplicative information requests are eliminated.*
- *Banks can stay focused on serving their customers.*

As such, this KYC-managed service enables banks and their customers to execute their responsibilities in a more-efficient, compliant, and cost-effective manner.[84]

---

[81] BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
[82] CPMI. 2016. Correspondent Banking.
[83] The World Bank Group. 2018. The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions.
[84] https://blogs.thomsonreuters.com/answerson/south-africa-leads-way-know-customer-kyc-compliance/

Annex 2: Recent Developments in Correspondent Banking

Qualitative Analysis

During the informal fact-finding carried out by the Committee on Payment and Market Infrastructures (CPMI) working group, the following correspondent banking trends were identified[85]:

- *Correspondent banking relationships are being reduced in number, especially for respondent banks that:*
  - *Do not generate sufficient volumes to recover compliance costs;*
  - *Are located in jurisdictions perceived to be too risky;*
  - *Provide payment services to customers about whom the necessary information for an adequate risk assessment is not available; and*
  - *Offer products or services or have customers that pose a higher risk for anti-money laundering/countering the financing of terrorism (AML/CFT) and therefore are more difficult to manage.*
- *Nested correspondent banking and payable-through accounts perceived to have higher associated risks are being scaled back so that traditional correspondent banking clearly predominates in the remaining relationships.*
- *Cutbacks in the number of relationships as well as changes in their nature have resulted in a significant concentration of relationships in a relatively small number of service-providing institutions that increasingly dominate this market.*
- *The establishment and maintenance of a correspondent banking relationship are perceived to be increasingly costly both for correspondent and respondent banks.*
- *Some correspondent banks are increasingly reluctant to provide correspondent banking services in certain foreign currencies in which the perceived risk of economic sanctions, the regulatory burden related to AML/CFT, or the uncertainties related to the implementation of these requirements and the potential reputational risk in case of noncompliance seem to be higher.*
- *Not all jurisdictions and currencies are affected equally. Respondent banks, in particular smaller banks located in jurisdictions perceived to be too risky, are especially affected by the reduction in the number of relationships.*

The drivers of de-risking are multiple and interrelated. Increasing costs, regulatory requirements, and an increased perception of risk are reducing the profit margins associated with this activity in some countries and/or with some customers and could be making this line of business increasingly unappealing to a growing number of correspondent banks. In particular, this is a business highly influenced by economies of scale, where banks are struggling to make returns when the business volumes in certain jurisdictions and/or with certain customers are not considered to justify the compliance costs involved. The perception is that this line of business has shifted from being a low-risk/low-margin segment to a high-risk/low-margin one.

SWIFT Quantitative Data Analysis

Monthly transaction data, provided by SWIFT on an exceptional basis, were used to analyze developments in correspondent banking quantitatively from 2011 to 2015[86]. The data contained sent and received volumes and nominal values for each country pair (corridor). The data included the number of active correspondents for each corridor in a given month. The data set contained information on more than 200 countries and territories. Because SWIFT is the most commonly used standard for cross-border payments, the data presumably captured a large part of correspondent banking activity.

When looking at aggregated data, the dominance of high-traffic corridors masks developments within other corridors and even entire regions with less significant activity. The data showed that payment traffic is concentrated in the

[85] Excerpt from CPMI. 2016. Correspondent Banking.
[86] Excerpt from CPMI. 2016. Correspondent Banking.

triangle linking Europe (without Eastern Europe) with Asia and North America. Therefore, the overall development can bias the picture because regional and national developments can differ substantially.

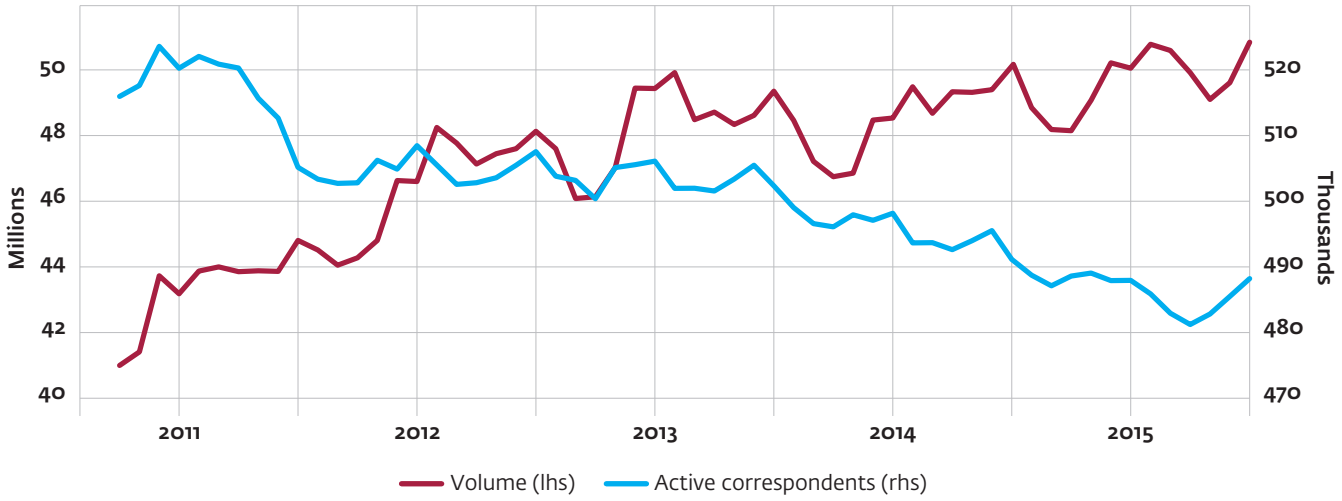
Overall volumes increased from 2011 to 2015 (see graph that follows). This is consistent with reports of de-risking in correspondent banking because payments are most likely switched to other channels after account closures. If payments are rerouted through third countries, this could even lead to an increase in correspondent banking activity. The graph that follows also shows a clear downward trend in the number of active correspondents across regions. Taken together, the falling number of active correspondents and the rise in volume suggest that concentration in correspondent banking has increased.

The downward trend in the number of active correspondent banks was confirmed in most cases at the regional level although with uneven dynamics. The data showed that the most pronounced absolute decline in active correspondents has occurred in European regions. Significant declines occurred in 2012, 2014, and 2015, whereas 2013 was often characterized by steady or even increases in activity.

Overall, the analysis showed that there has been a trend toward concentration in correspondent banking activity as measured by payment traffic. This is consistent with findings from survey data by the World Bank (2015).

For additional information on developments in correspondent banking, outside of this publication, refer to "Developments in Correspondent Banking." (In Correspondent Banking, pp 9–17. Basel, Switzerland: Bank for International Settlements, Committee on Payment and Market Infrastructures, 2016.)

Figure 11: Transaction Volume by number of SWIFT messages



Sources: Deutsche Bundesbank; SWIFT Watch

Annex 3: List of Most Relevant Financial Action Task Force Recommendations and Basel Publications

Financial Action Task Force (FATF) Recommendations

R. 1 Assessing risks and applying a risk-based approach

R. 2 National cooperation and coordination

R. 9 Financial institution secrecy law

R. 10 Customer due diligence

R. 11 Recordkeeping

R. 12 Politically exposed persons

R. 13 Correspondent banking

R. 15 New technologies

R. 16 Wire transfers

R. 17 Reliance on third parties

R. 18 Internal controls and foreign branches and subsidiaries

R. 20 Reporting of suspicious transactions

R. 21 Tipping-off and confidentiality

R. 24 Transparency and beneficial ownership of legal persons

R. 25 Transparency and beneficial ownership of legal arrangements

R. 26 Regulation and supervision of financial institutions

Basel Publications

1. *Sound Management of Risks Related to Money Laundering and Financing of Terrorism (2017)*
2. *Corporate Governance Principles for Banks (2015)*

Annex 4: General Guide to Account Opening

This guide is meant to be a tool for banks to use when opening a new customer account. Although it does not cover all instances that may occur, it can help banks develop their customer identification and verification programs and includes information that should be collected and verified at account opening for natural persons,[87] legal persons,[88] and legal arrangements.[89] It is understood that in developed markets this information is often readily available, but this may not be the case in many emerging markets. Proof of residential address, for example, is one piece of information that is usually problematic especially for clients from rural areas and those cities/towns where no formal addressing system exists.

COLLECTION OF INFORMATION

To the extent practicable, banks should collect the following information for identification purposes from the customer or other available source[90]:

	Natural Persons	Legal Persons	Legal Arrangements
At a minimum [a]	• Legal name (first and last name); • Complete residential address;[b] • Nationality, an official personal identification number or other unique identifier;[b] • Date and place of birth.[b]	• Name, legal form, status and proof of incorporation of the legal person; • Permanent address of the principal place of the legal person's activities; • Official identification number (company registration number, tax identification number); • Mailing and registered address of legal person; • Identity of natural persons who are authorized to operate the account. In the absence of an authorized person, the identity of the relevant person who is the senior managing official; • Identity of the beneficial owners; • Powers that regulate and bind the legal person (such as the articles of incorporation for a corporation).	• Name of the legal arrangement and proof of existence; • Address and country of establishment; • Nature, purpose, and objects of the legal arrangement (for example, discretionary or testamentary); • The names of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (including through a chain of control/ownership).

[87] Natural persons are individuals who are customers or beneficial owners or authorized signatories.
[88] FATF defines "legal persons" as any entities other than natural persons that can establish a permanent customer relationship with a bank or otherwise own property. This can include companies, bodies corporate, foundations, Anstalt-type structures, partnerships, or associations and other relevantly similar entities.
[89] FATF defines "legal arrangements" as express trusts or other similar arrangements.
[90] Excerpt from BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

Potential additional information (on the basis of risks)	• Any other names used (such as marital name, former legal name, or alias); • Business address, post office box number, e-mail address and landline or mobile telephone numbers; • Residency status;[c] • Gender.[c]	• Legal entity identifier (LEI), if eligible;[d] • Contact telephone and fax numbers; • Identity of relevant persons holding senior management positions.	• LEI, if eligible;[d] • Contact telephone and fax numbers if relevant; • The names of the relevant persons having a senior management position in the legal arrangement, if relevant, addresses of trustees, beneficiaries.

a Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The table does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

b There are circumstances when this information is legitimately unavailable. This could prevent the clients from accessing formal banking services. If clients are allowed to access to formal banking services, banks should apply mitigating measures as provided for by their internal risk policies, in line with national laws. Such measures could include utilizing alternative information or conducting appropriate monitoring.

c The collection of this information may be subject to national data protection and privacy regimes.

d Subject to developments in the LEI project, this information may become required in the future.

Banks should collect the following additional information to develop an initial customer risk profile:

	Natural Persons	**Legal Persons**	**Legal Arrangements**
At a minimum[a]	• Occupation, public position held; • Income; • Expected use of the account: amount, number, type, purpose and frequency of the transactions expected; • Financial products or services requested by the customer.	• Nature and purpose of the activities of the legal entity and its legitimacy; • Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	• Description of the purpose/ activities of the legal arrangement (for example, in a formal constitution, trust deed); • Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.
Potential additional information (on the basis of risks)	• Name of employer, where applicable; • Sources of customer's wealth; • Sources of funds passing through the account; • Destination of funds passing through the account.	• Financial situation of the entity; • Sources of funds paid into the account and destination of funds passing through the account.	• Source of funds; • Origin and destination of funds passing through the account.

a Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The table does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

VERIFICATION OF CUSTOMER IDENTITY

Banks should verify the identity of the customer established through information that was collected for identification purposes using reliable, independently sourced documents, data, or information[91]. All measures used to verify the identity of the customer should be proportionate to the risk posed by the customer relationship and should enable the bank to satisfy itself that it knows who the customer is. Verification can be completed using documentary and nondocumentary procedures. Below are some examples of different verification procedures. This list of examples is not exhaustive.

[91] Excerpt from BCBS. 2017. Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism.

	Natural Persons	Legal Persons	Legal Arrangements
Documentary verification procedures	• Confirming the identity of the customer or the beneficial owner from an unexpired official document (for example, passport, identification card, residence permit, Social Security records, or driver's license) that bears a photograph of the customer; • Confirming the date and place of birth from an official document (for example, birth certificate, passport, identity card, or Social Security records); • Confirming the validity of official documentation provided through certification by an authorized person (for example, embassy official or public notary); • Confirming the residential address (for example, utility bill, tax assessment, bank statement, or letter from a public authority).	• Obtaining a copy of the certificate of incorporation and memorandum and articles of association or partnership agreement (or any other legal document certifying the existence of the entity, such as abstract of the registry of companies/commerce); • For established corporate entities, reviewing a copy of the latest financial statements (audited, if available).	• Obtaining a copy of documentation confirming the nature and legal existence of the account holder (for example, a deed of trust or register of charities).
Nondocumentary verification procedures	• Contacting the customer by telephone or letter to confirm the information supplied, after an account has been opened (for example, a disconnected phone or returned mail should warrant further investigation); • Checking references provided by other financial institutions; • Using an independent information verification process, such as by accessing public registers, private databases, or other reliable independent sources (for example, credit reference agencies).	• Undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been or is not in the process of being dissolved, struck off, wound up or terminated; • Using an independent information verification process, such as by accessing public corporate registers, private databases, or other reliable independent sources (for example, lawyers or accountants); • Validating the LEI and associated data in the public access service; • Obtaining prior bank references; • Visiting the corporate entity, where practical; • Contacting the corporate entity by telephone, mail, or e-mail.	• Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted; • Obtaining prior bank references; • Accessing or searching public and private databases or other reliable independent sources.

a Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The table does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

For additional guidance on account opening, outside of this publication, refer to "Annex 4: General Guideline to Account Opening." (In Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism, pp. 33–43. Basel, Switzerland: Bank for International Settlements, Basel Committee on Banking Supervision (BCBS), 2017.)

Annex 5: Wolfsberg Guidelines

The Wolfsberg Group is an association of 13 global banks that aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to know your customer (KYC) and anti-money laundering/countering the financing of terrorism (AML/CFT) policies. Materials published by the Wolfsberg Group are designed to provide financial institutions with an industry perspective on effective financial crime risk management.

The Wolfsberg Group has published multiple materials in the form of principles, guidance, frequently asked questions, and statements, all of which can be found on the Group's website (https://www.wolfsberg-principles.com). Listed here are some of the key documents published by the Group in recent years that are designed to promote the effectiveness of AML/CFT programs:

- *Correspondent Banking Due Diligence Questionnaire (2018);*[92]
- *Country Risk Frequently Asked Questions (2018);*[93]
- *Payment Transparency Standards (2017);*[94]
- *Guidance on Politically Exposed Persons (2017);*[95]
- *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption (2015);*[96]
- *Anti-Money Laundering Principles for Correspondent Banking (2014);*[97]*and*
- *Frequently Asked Questions on Correspondent Banking (2014).*[98]

[92] https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%27s_CBDDQ_140618_v1.2.pdf
[93] https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20FC%20Country%20Risk%20FAQs%20Mar18.pdf
[94] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf
[95] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/4.%20Wolfsberg-Guidance-on-PEPs-May-2017.pdf
[96] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf
[97] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf
[98] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/18.%20Wolfsberg-Correspondent-Banking-FAQ-2014.pdf

Creating Markets, Creating Opportunities